
AWS
re:Invent
DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

SEC203-INT

Security insights and innovation from AWS

Chris Betz
Chief Information Security Officer,
AWS

Becky Weiss
VP and Distinguished Engineer,
AWS

Rodrigo Castillo
CTO,
Commonwealth Bank of Australia

Jason Clinton
Chief Information Security Officer,
Anthropic

Chris Betz

Chief Information Security Officer, AWS

Security is our **top priority**.

CULTURE OF SECURITY:

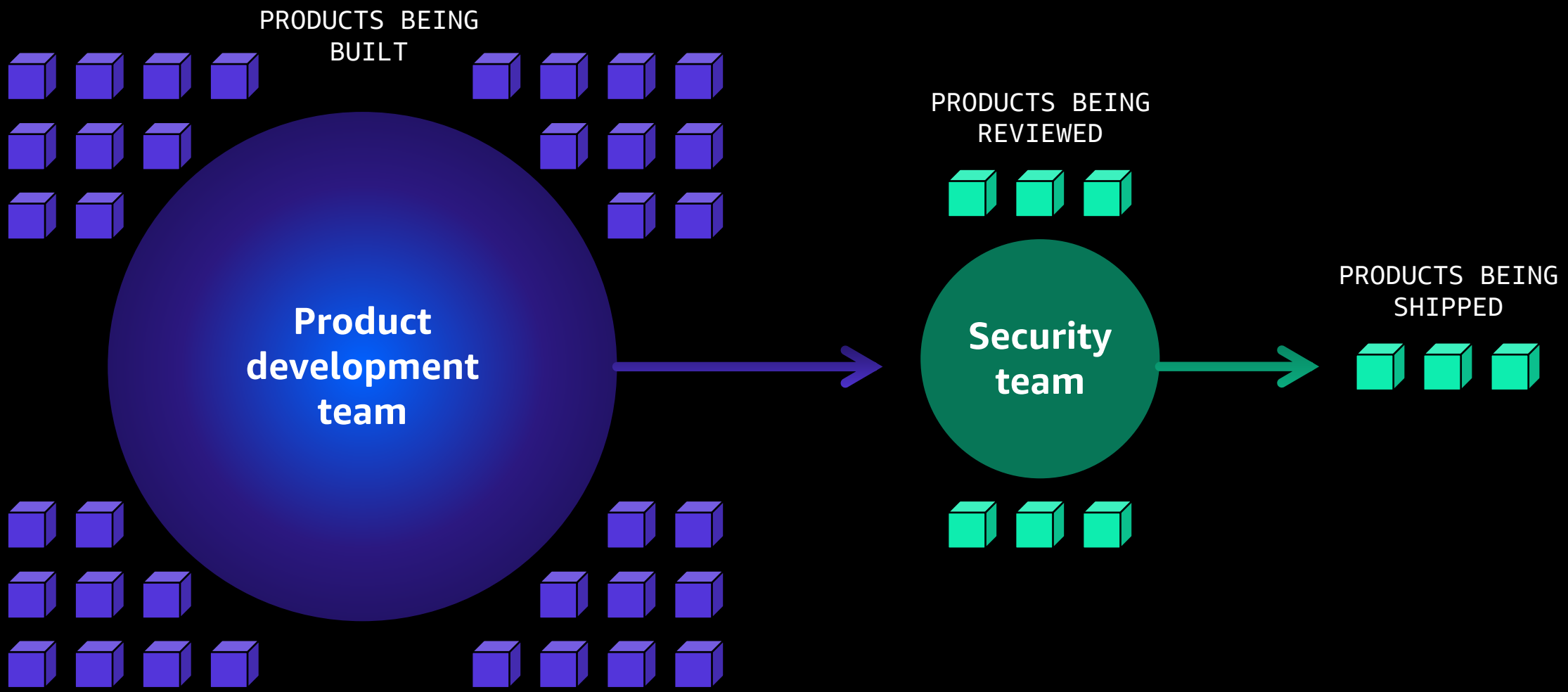
The knowledge, values, and norms shared by members of an organization that **affect its security**

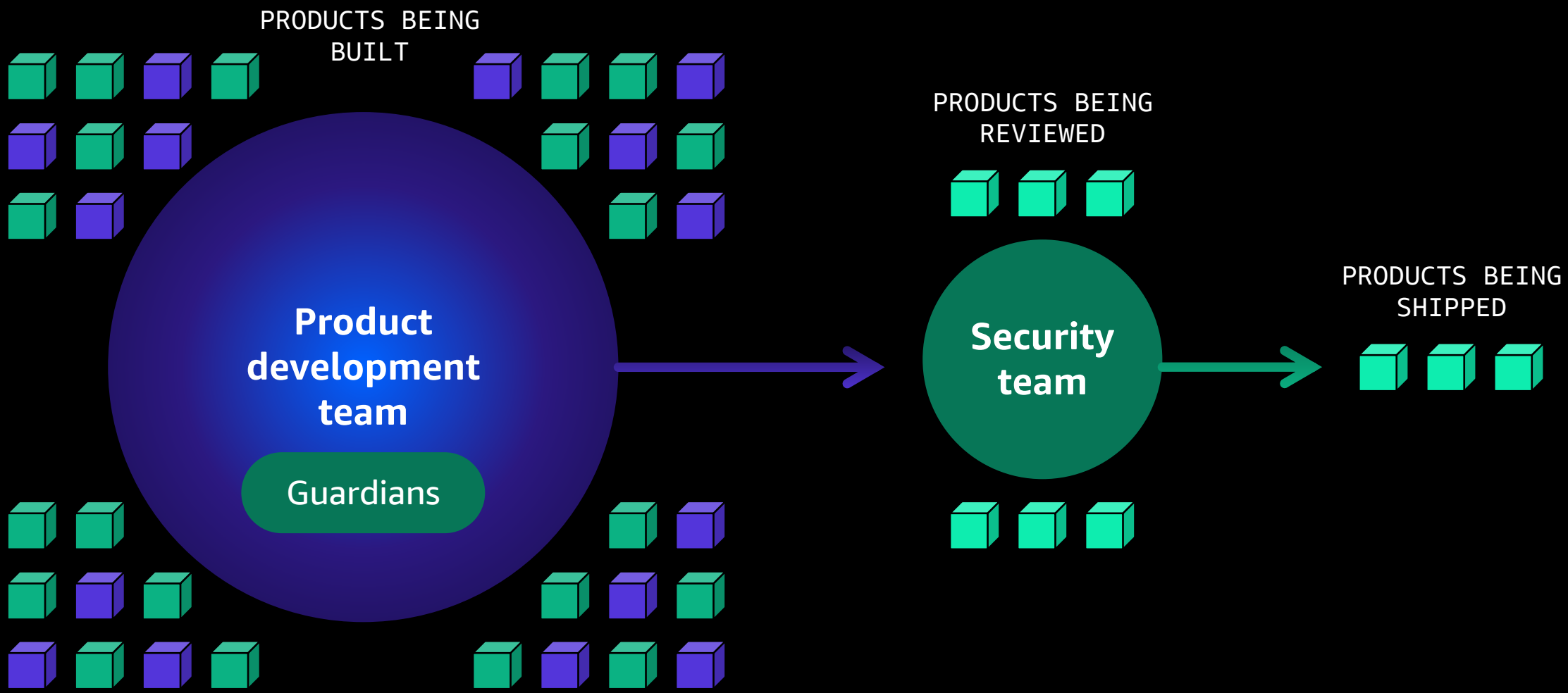
Leaders are owners. They think long term and don't sacrifice long-term value for short-term results. They act on behalf of the entire company, beyond just their own team. They never say "that's not my job."

Amazon Leadership Principles

Embracing escalation

We **distribute** security expertise.





5,000

BUILDERS TRAINED

Launch products that are secure by design

22%

FEWER REVIEW FINDINGS

Identify risks and findings sooner

20%

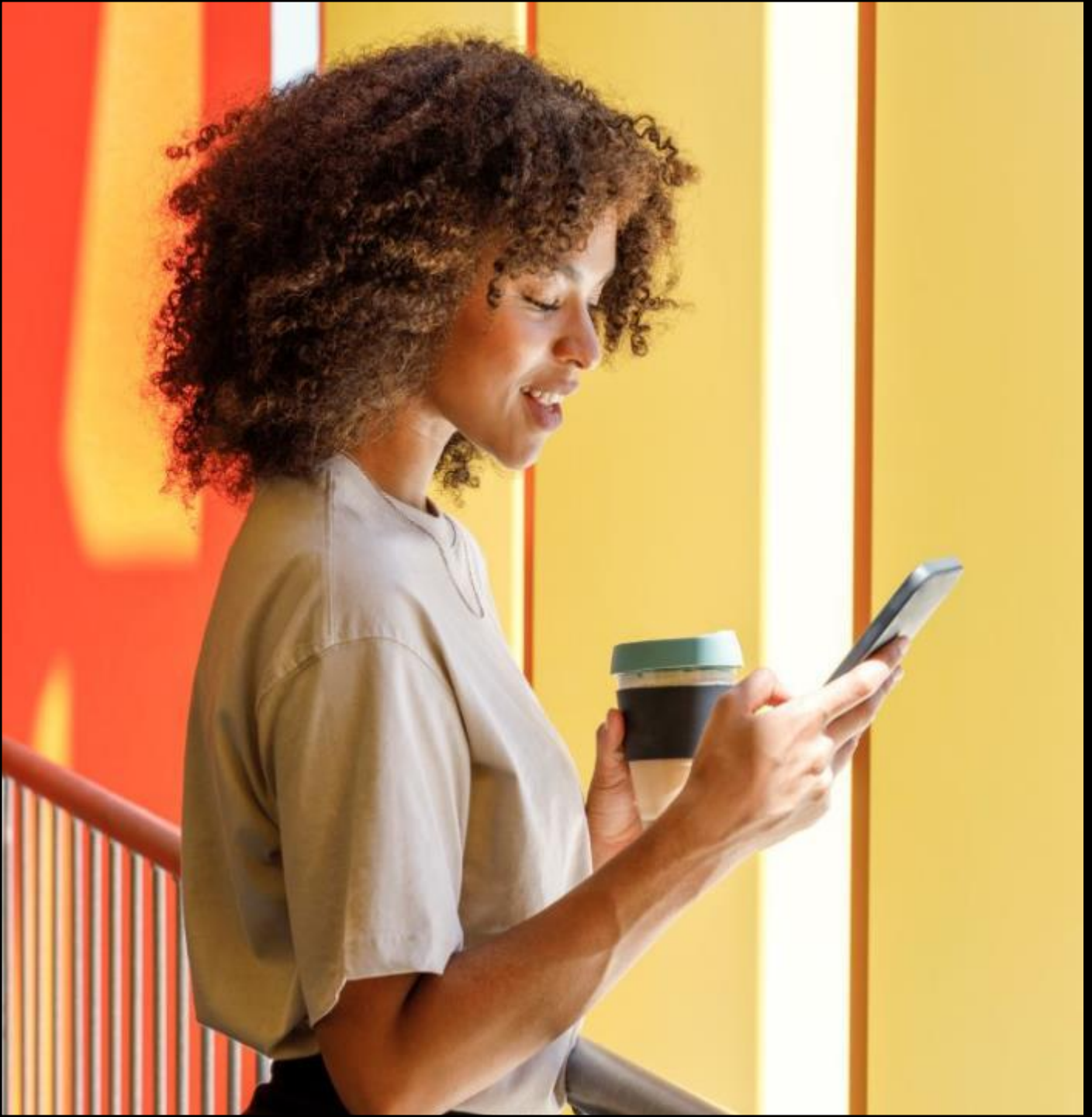
FASTER REVIEWS

Launch on schedule, with a high security bar

Rodrigo Castillo

Chief Technology Officer,
Commonwealth Bank of Australia

DevSecOps Transformation
Our cultural approach



Building tomorrow's bank today for our customers

Commonwealth Bank

Our Technology Strategy

An organisation primed for delivery

A modern technology estate

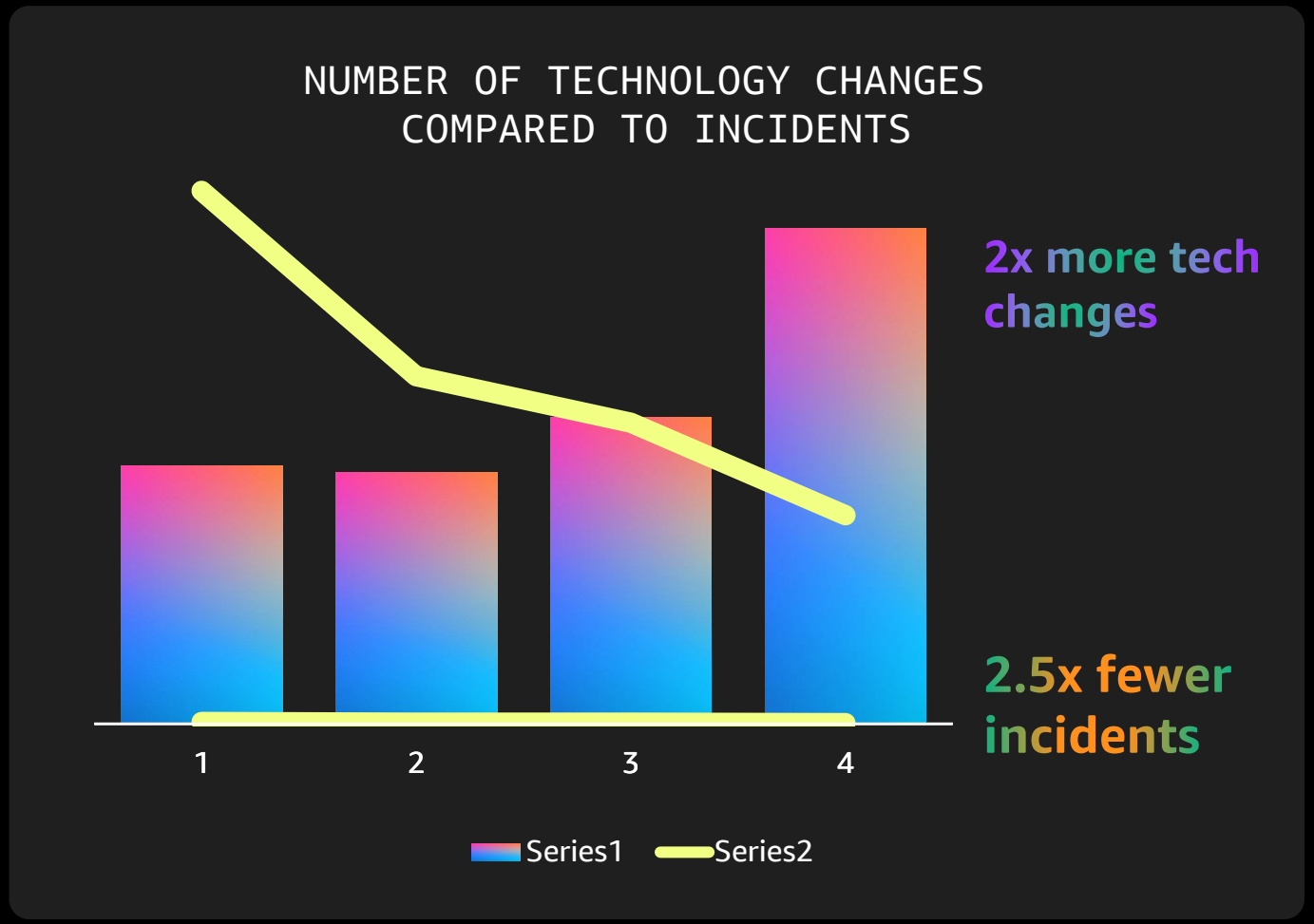
World-class data and AI

Best-in-class security, resiliency and reliability

Our DevSecOps and engineering platform transformation

Transformation outcomes:

- **Maturity Framework** embedded for 12 capabilities
- **Built-in controls** such as code quality and secure code scan
- **4x faster** cyber reviews in software and system development lifecycle



Security Academy

HIGHLIGHTS, UPDATES AND METRICS

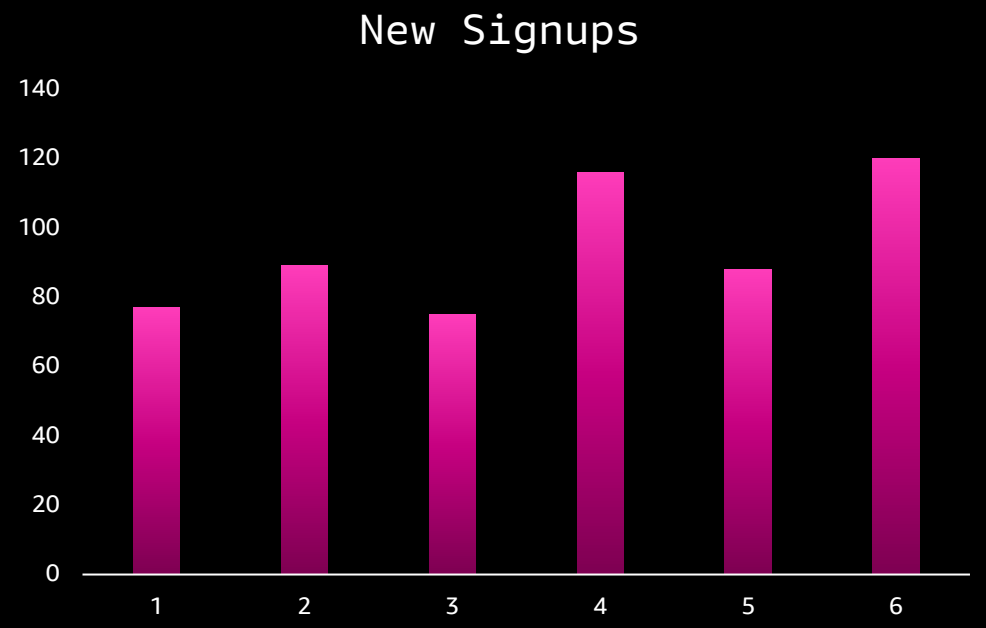
More than 1,500 total participants

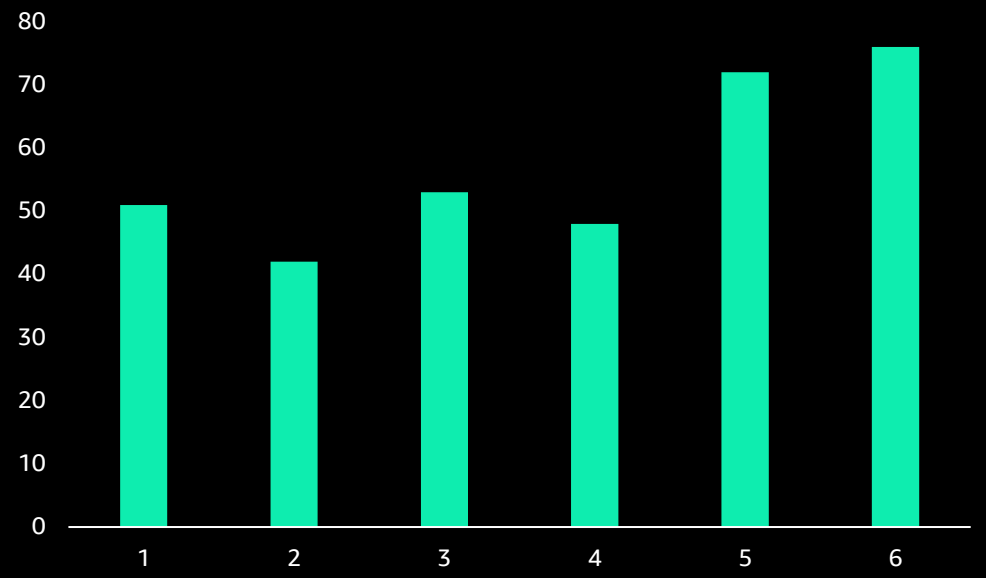
800+ Champions!

Majority of Security Design work completed by Security Champions

Security Academy 2.0 has been launched

- Security Core
- Security Design
- Cloud Security
- Application Security
- Security Operations

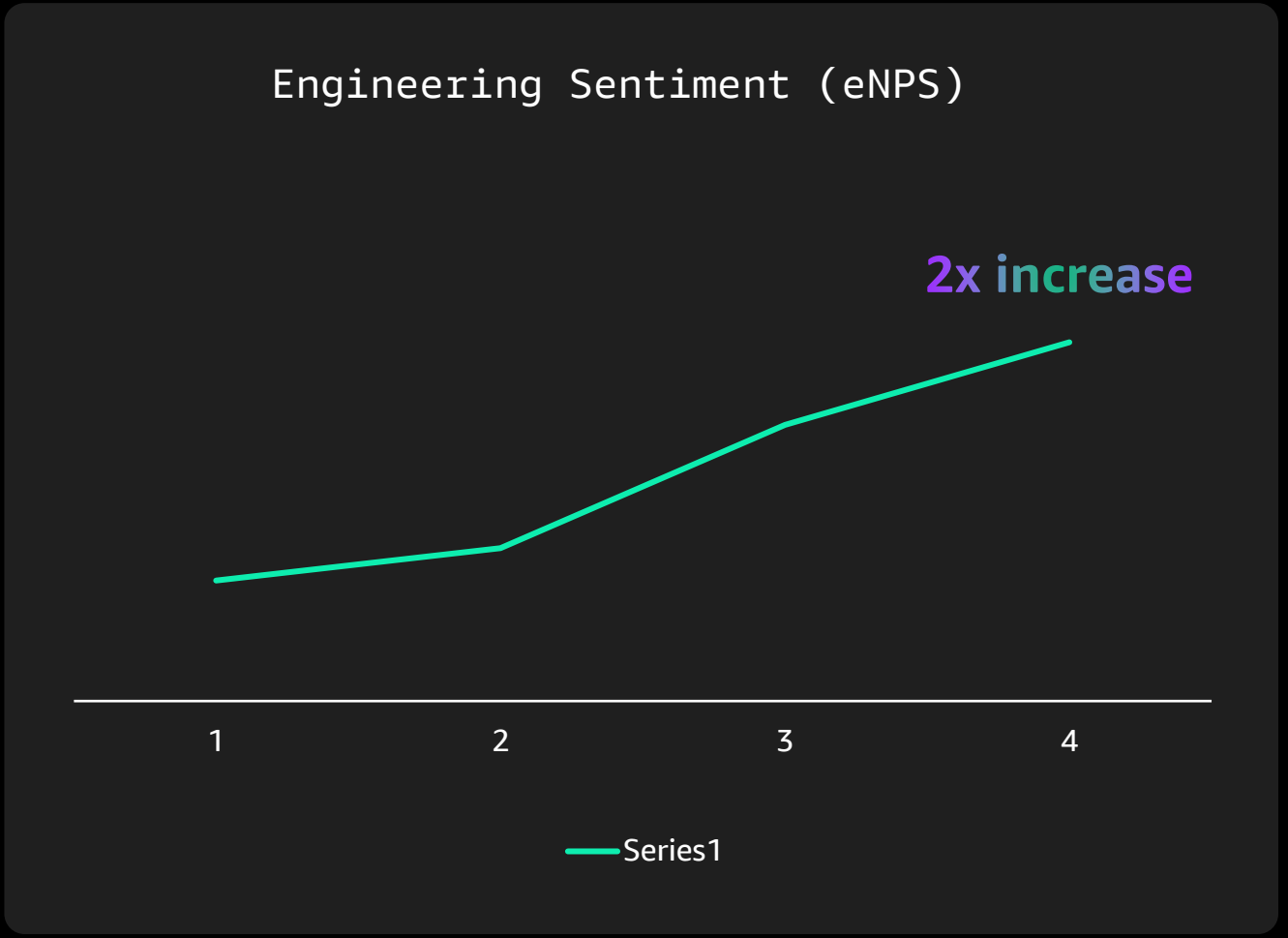




What our teams told us

Engineers feel more supported and able to manage their workloads:

- 67% of engineers feel they can work at a pace that does not contribute to incurring technical debt or security vulnerabilities
- 82% of engineers feel valued for their engineering skills in organisation



Cultural shifts

Blameless culture when finding root causes to important incidents.

A weekly Operational Review is held to discuss details of the incident root causes.

Secure by Design with our DevSecOps model.

All engineers are accountable end-to-end for the security of their services, rather than handing over to a different team.

Velocity and resiliency as a result, making it easier to make changes, develop new products and innovate for our customers.

Commonwealth Bank

Thank you!

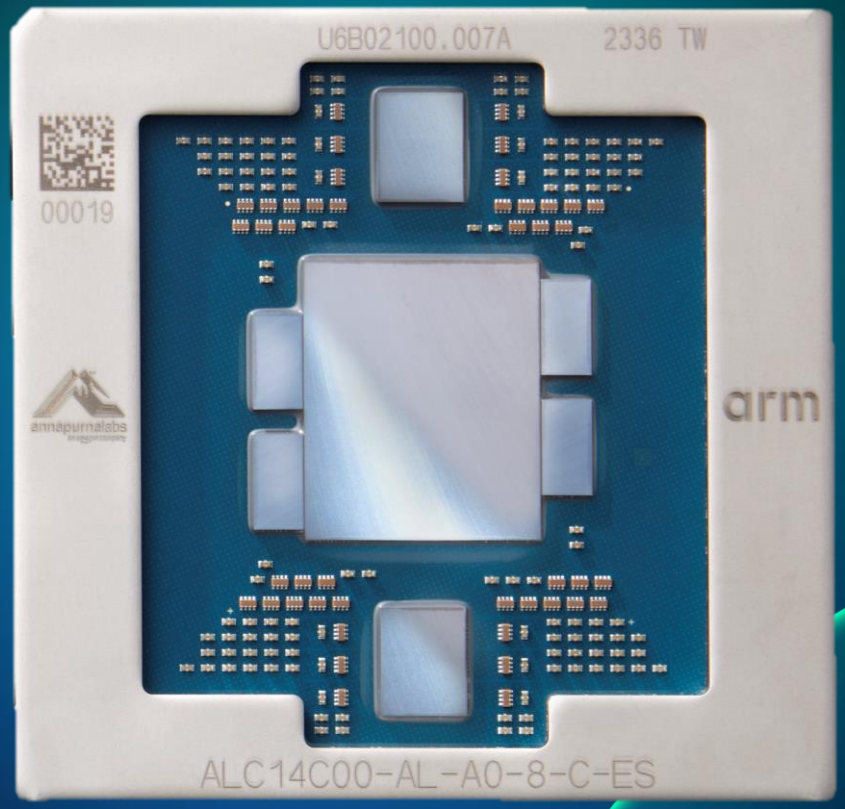
Rodrigo Castillo

Rodrigo.Castillo@cba.com.au

 linkedin.com/in/rodrigocastillof

We empower people
by scaling **security innovation**.

Secure by design
at the silicon level



GRAVITON4

GRAVITON4

Security enhancements

Full encryption of all high-speed physical interfaces

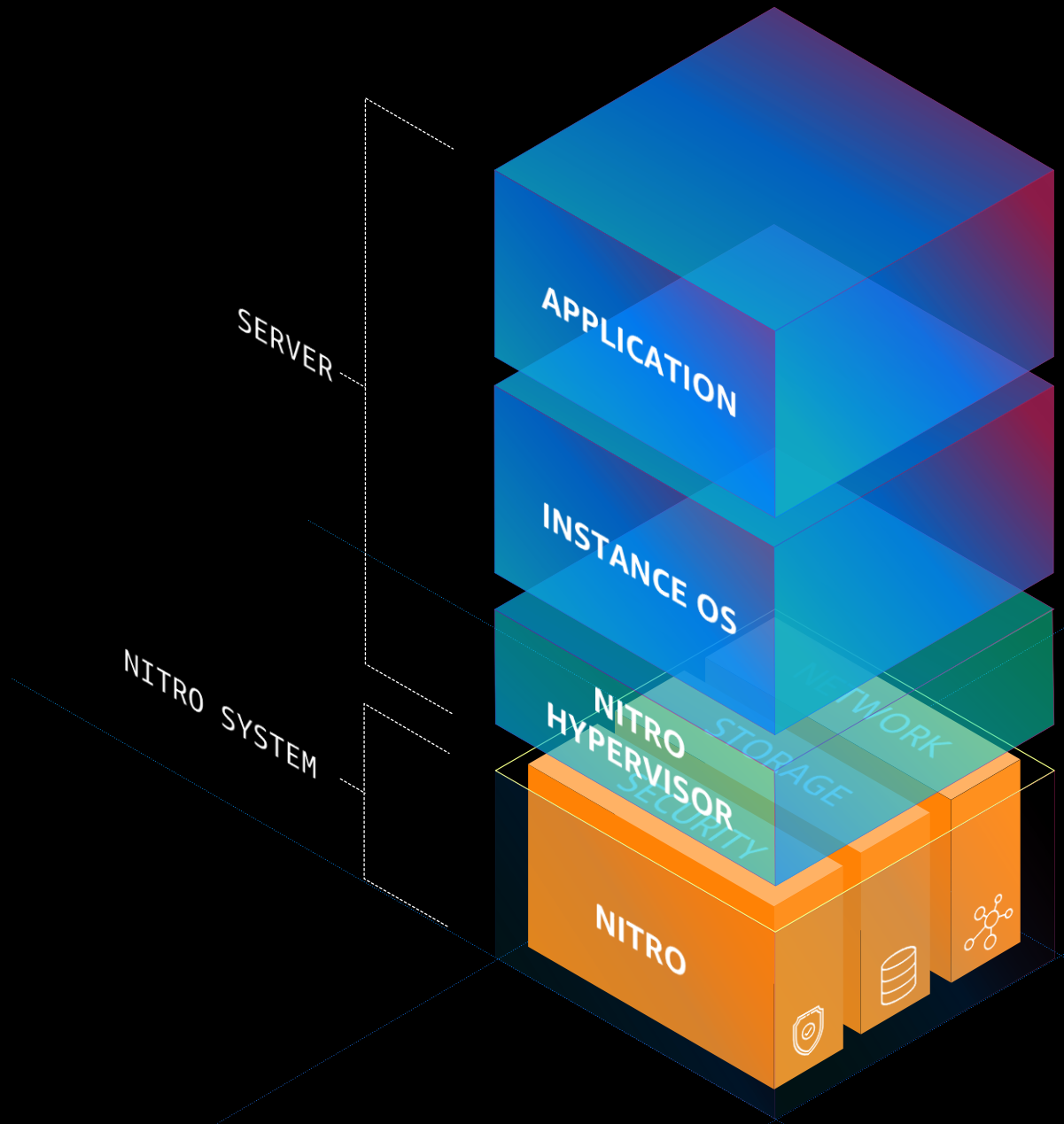
Pointer authentication

Branch target identification

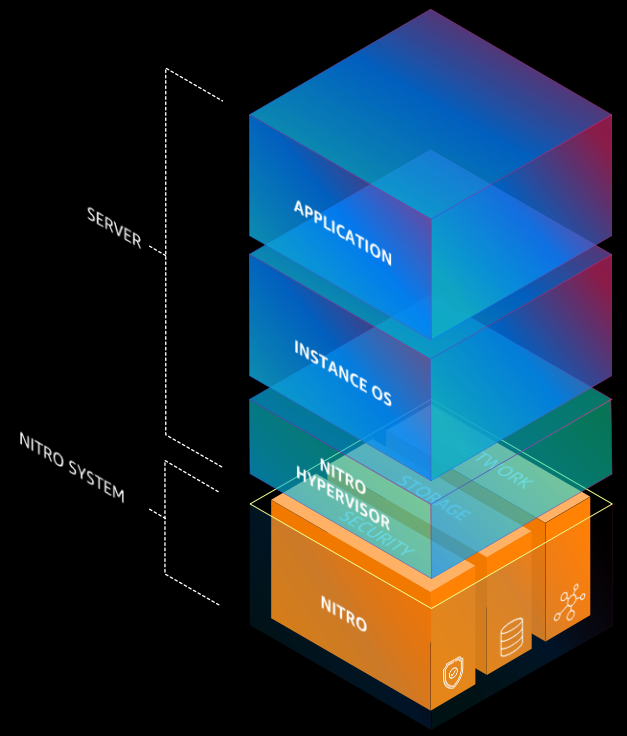
No simultaneous multi-threading (SMT)

The AWS Nitro System architecture

OFFERING THE BEST SECURITY, PERFORMANCE, AND INNOVATION IN THE CLOUD



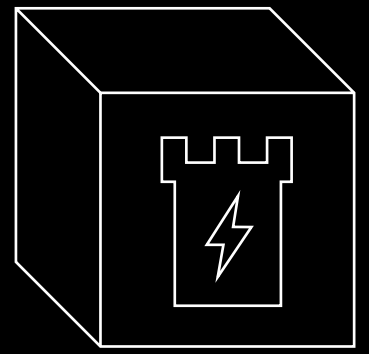
AWS Nitro System



Foundation of virtualization in modern Amazon EC2 instances

DIMENSION 1

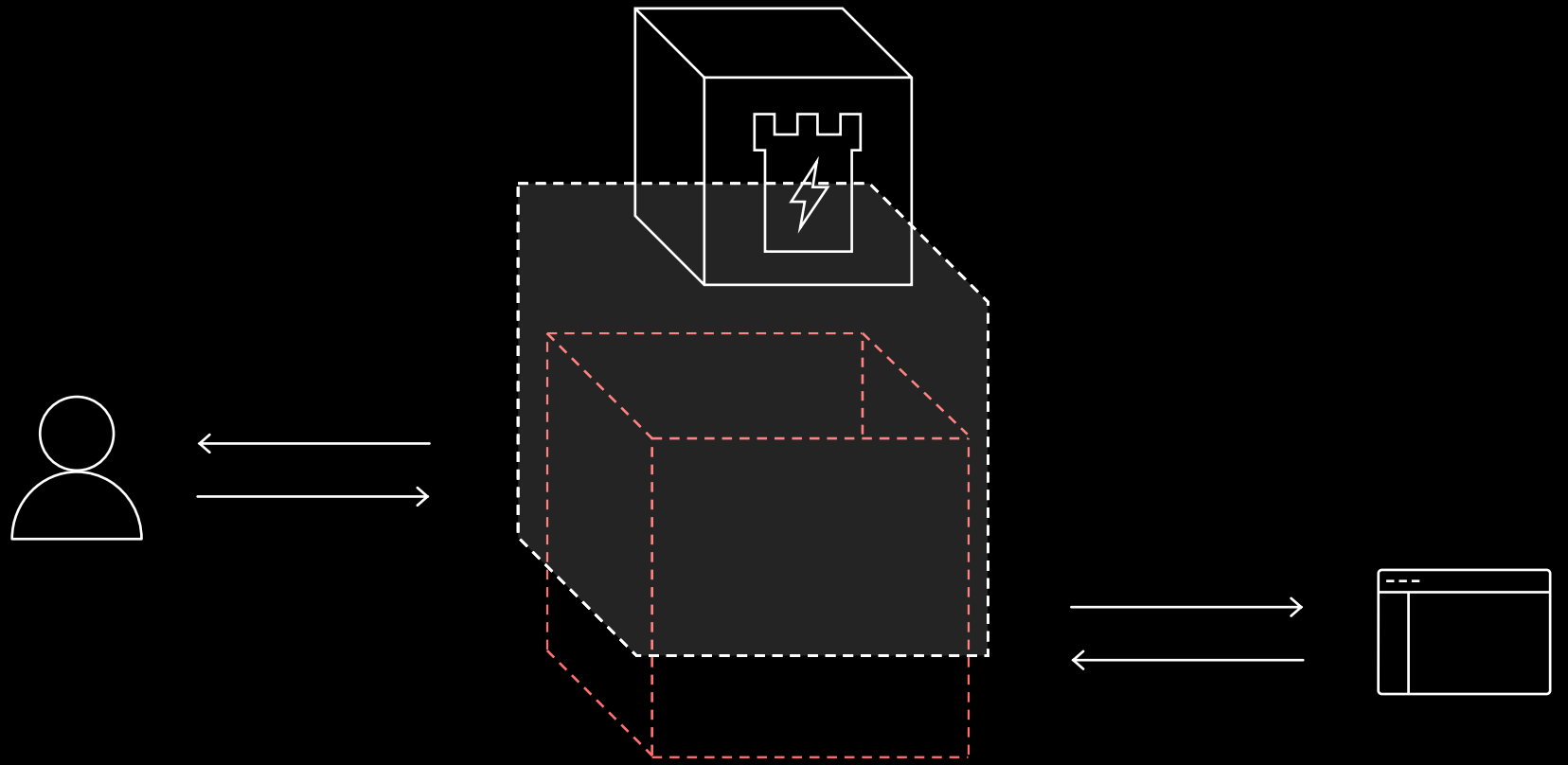
AWS Nitro Enclaves



Additional customer-level isolation with hardened, highly-isolated compute environment

DIMENSION 2

AWS Nitro Enclaves



The **evolution** of compute isolation

MicroVM (Guest OS & container workload)

Firecracker

KVM

Host

Firecracker

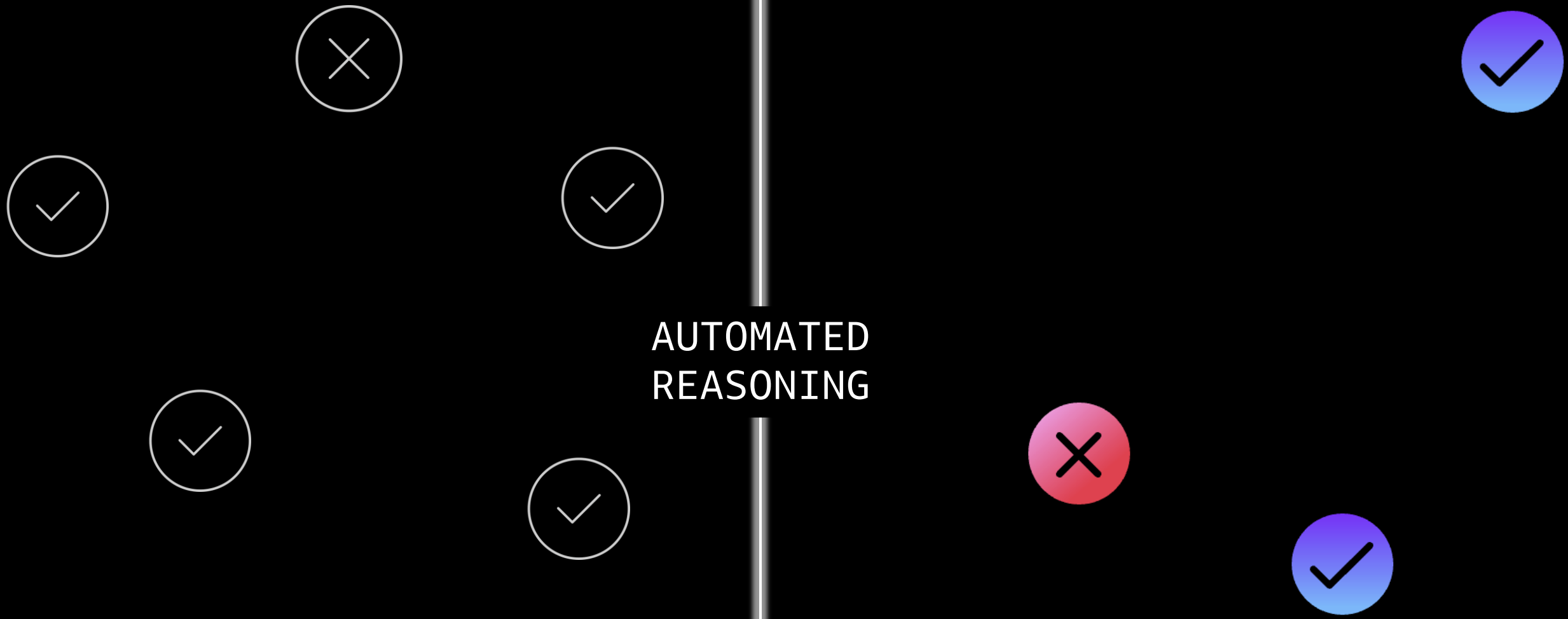
Restful API

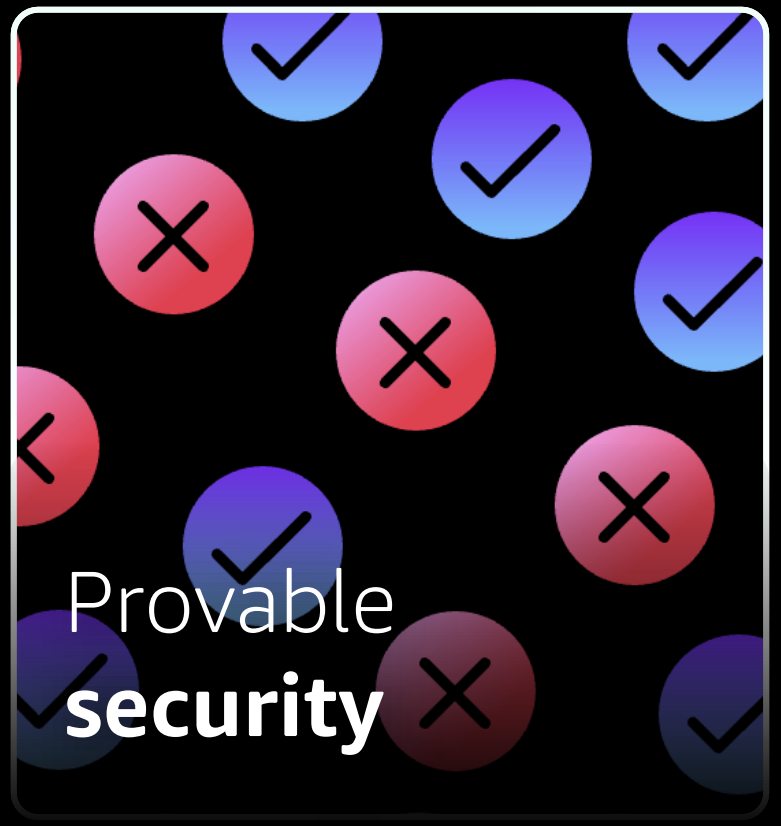
Networks

Storage

Rate limiting

Metadata service





Verify correctness

- CRYPTOGRAPHIC PROTOCOLS
- AUTHORIZATION LOGIC
- CONSISTENCY OF STORAGE SYSTEMS

Prove there is no unintended access

POLICY AND NETWORK CONTROL

Verify security mechanisms

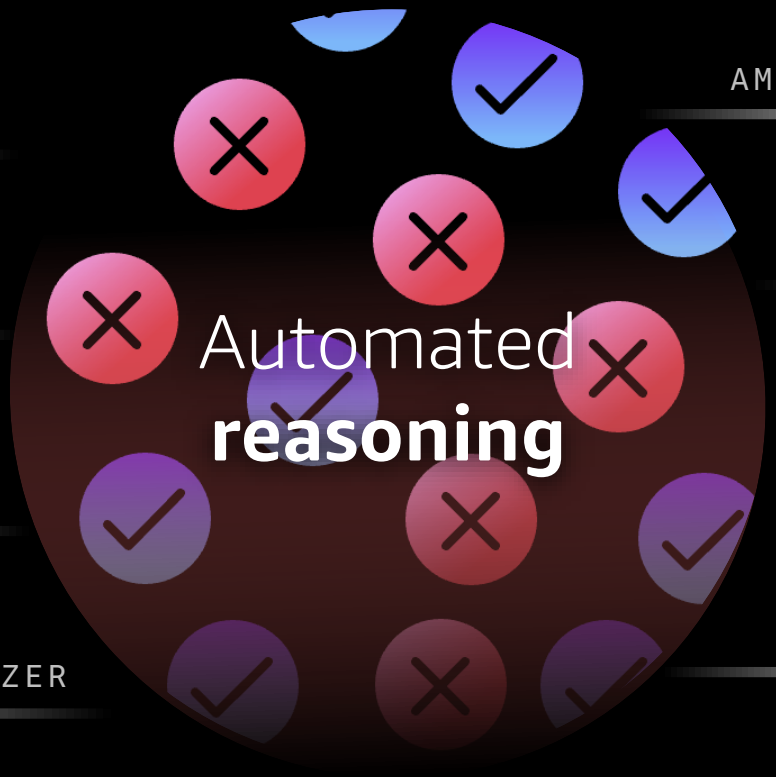
- FIREWALLS
- CLOUD GOVERNANCE
- CODING PRACTICES

AWS CONFIG MANAGED RULES

AMAZON S3 SUBSYSTEMS

AMAZON INSPECTOR
REACHABILITY RULES

VPC REACHABILITY ANALYZER



AMAZON CODEGURU

AWS IAM AUTHORIZATION ENGINE

AWS IAM ACCESS ANALYZER

CEDAR

Threat intelligence

Algorithms that help predict malicious domains before they appear in threat intel feeds

Processes over a trillion DNS requests a day

Discovers an average of 124,000 malicious domains a day

Intelligence integrated into Amazon GuardDuty

Threat disruption

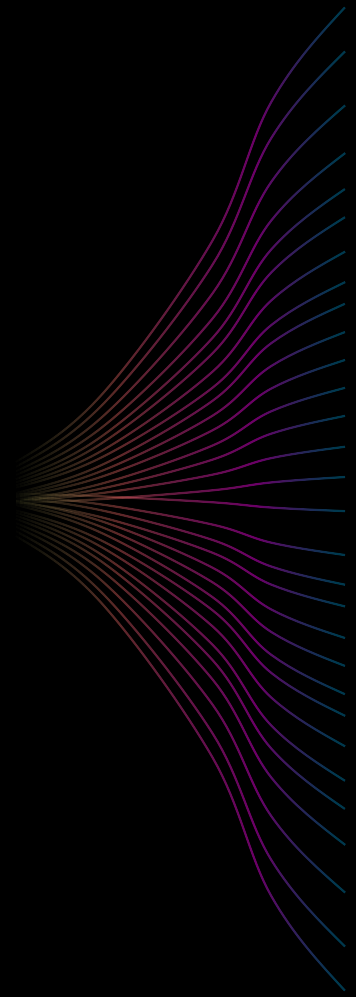
Network telemetry analyzer that detects and restrict suspicious behavior within minutes

More than **27 billion** attempts to find unintentionally public S3 buckets

Nearly **2.7 trillion** attempts to probe Amazon EC2 instances

Automated protections in Amazon S3, Amazon VPC, AWS Shield, and AWS WAF

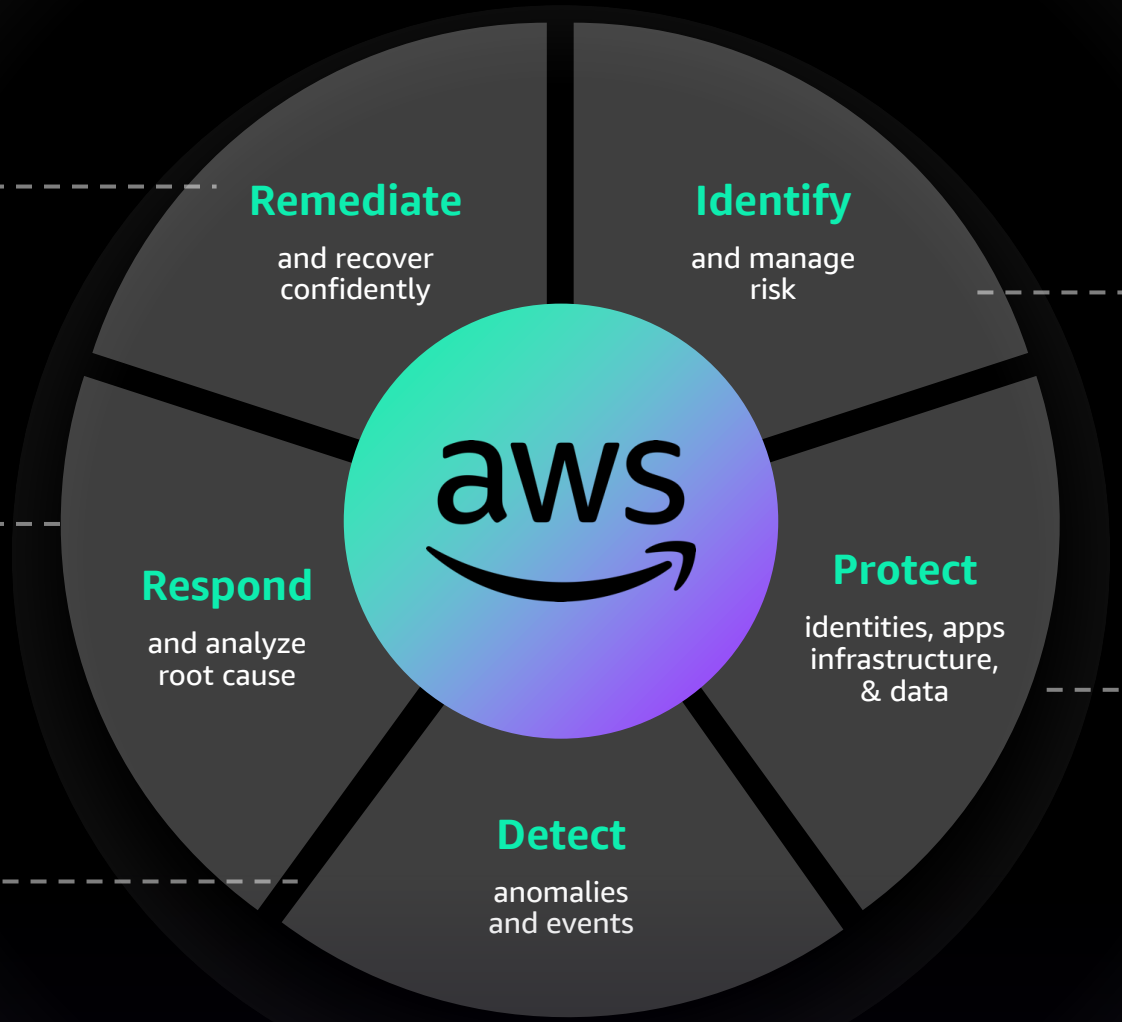
Threat intelligence



- AWS Shield
- Amazon GuardDuty
- Amazon S3
- AWS WAF
- AWS Network Firewall
- Amazon Route 53 Resolver DNS Firewall
- Amazon VPC

AWS foundational and layered security services

- Automated recovery
- Self-healing capabilities
- **Mechanisms to plan, test, and recover**



- Deep visibility
- **Governance that enables agility**
- +Compliance—risk assessment

- **Incident response**
- Root cause analysis
- Visualize security data

- **Network security posture management**
- Encrypt everything
- Fine-grained identity controls
- Comprehensive compliance controls
- **Core zero trust building blocks**

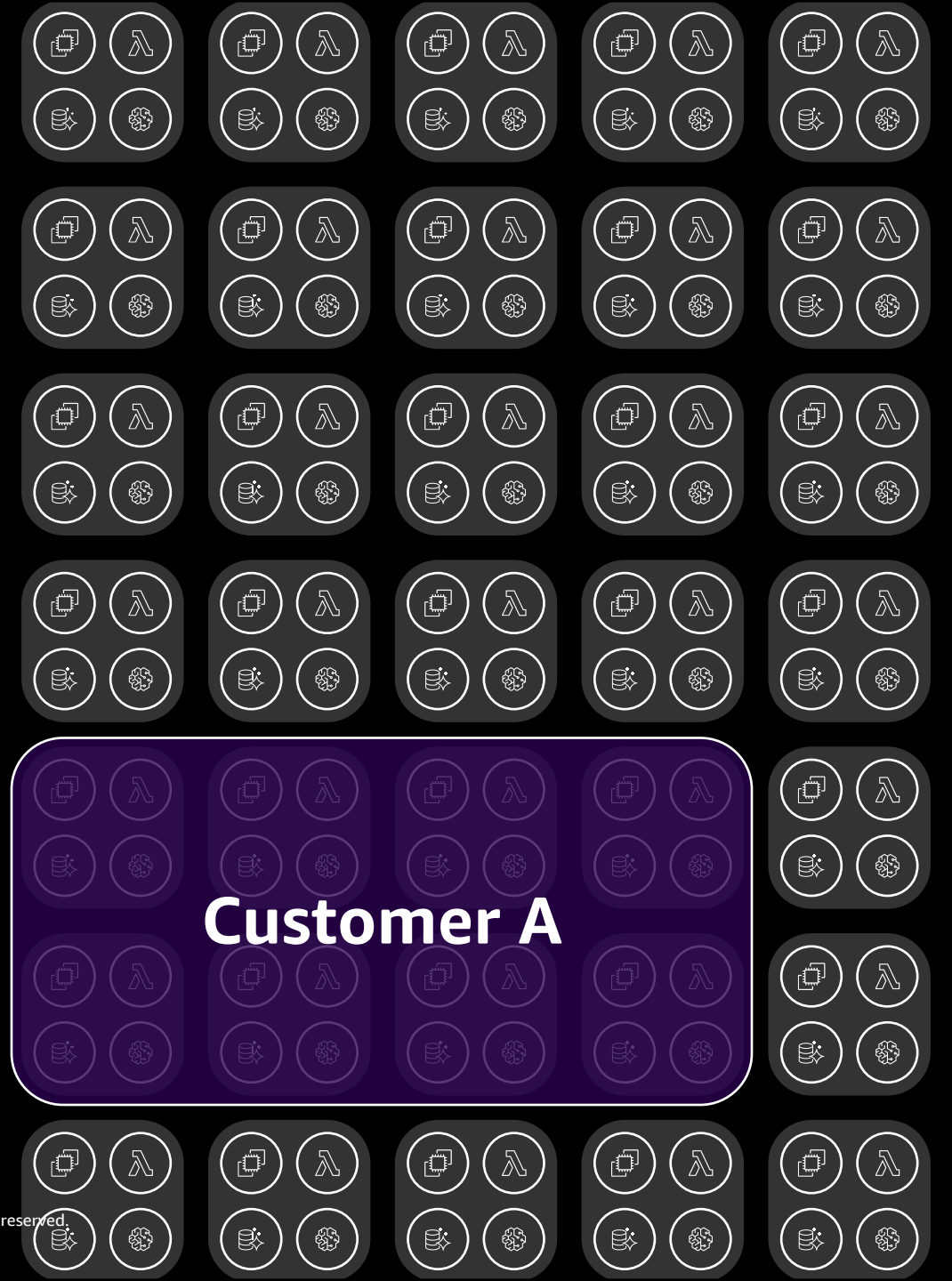
- Continuous monitoring
- **Threat intelligence**
- **Security automation**
- Automated compliance reporting

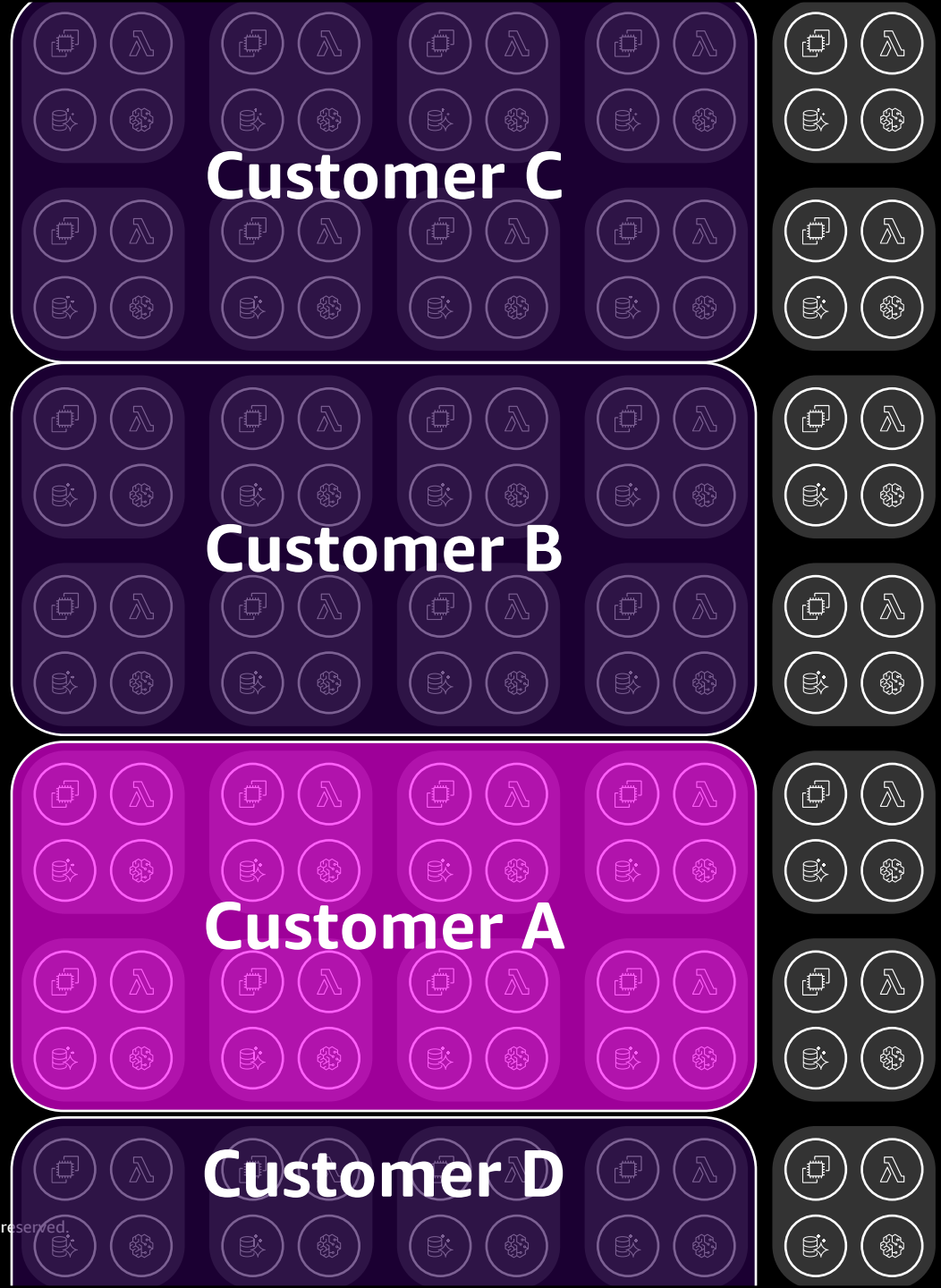
BUILT AND ARCHITECTED TO BE THE MOST SECURE CLOUD INFRASTRUCTURE

Becky Weiss

VP and Distinguished Engineer, AWS

AWS
Environment





No matter how large my AWS environment is,
or how many people are in my AWS environment,
or which AWS services I use –
it's **my identities**, accessing **my resources**,
from **my networks**.

GENERALLY AVAILABLE

NEW

Resource control policies

Build a data perimeter around AWS resources at scale

Centrally define and enforce consistent access controls on resources at scale

Restrict access to your resources with preventative controls

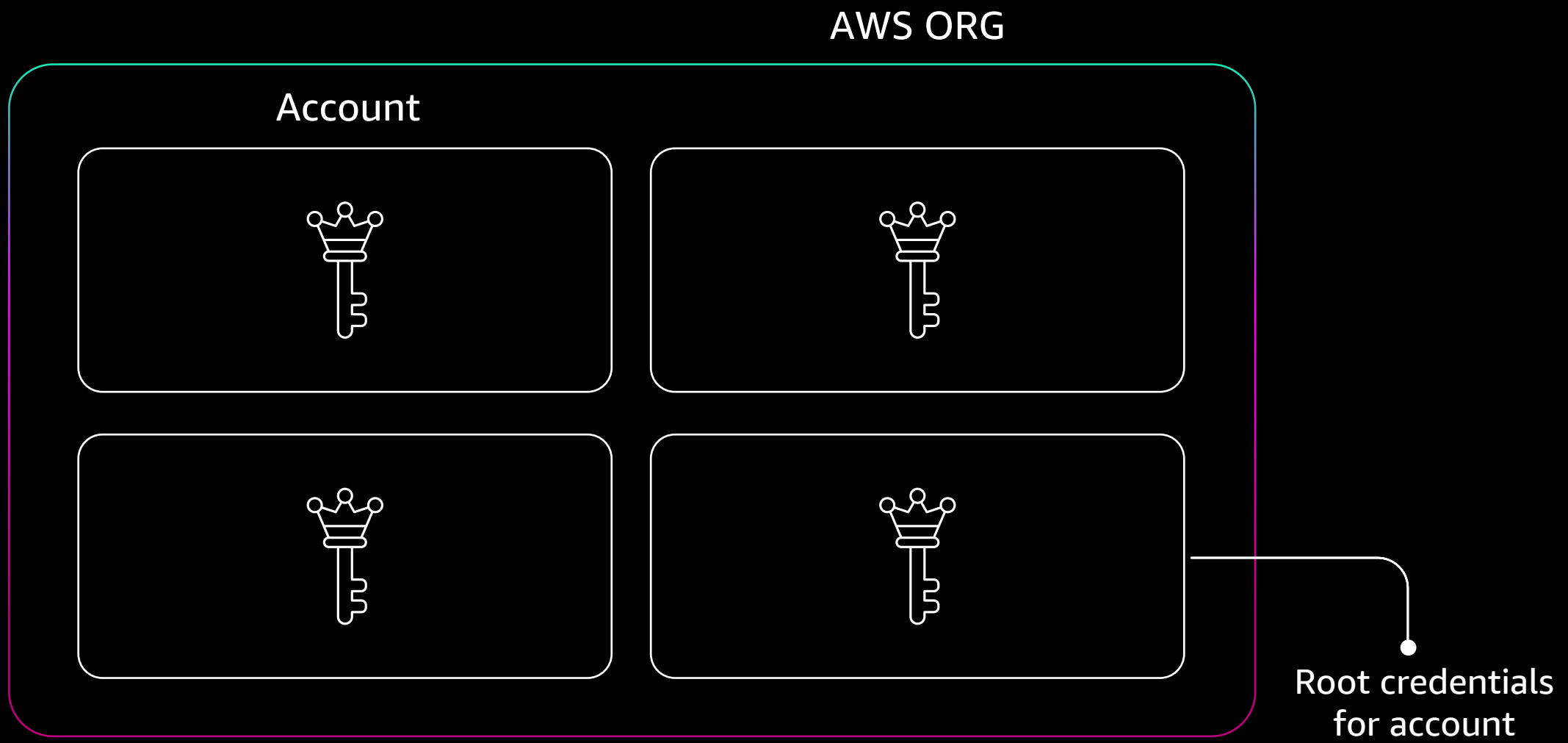
Empower your teams to innovate faster while staying secure

LEARN MORE

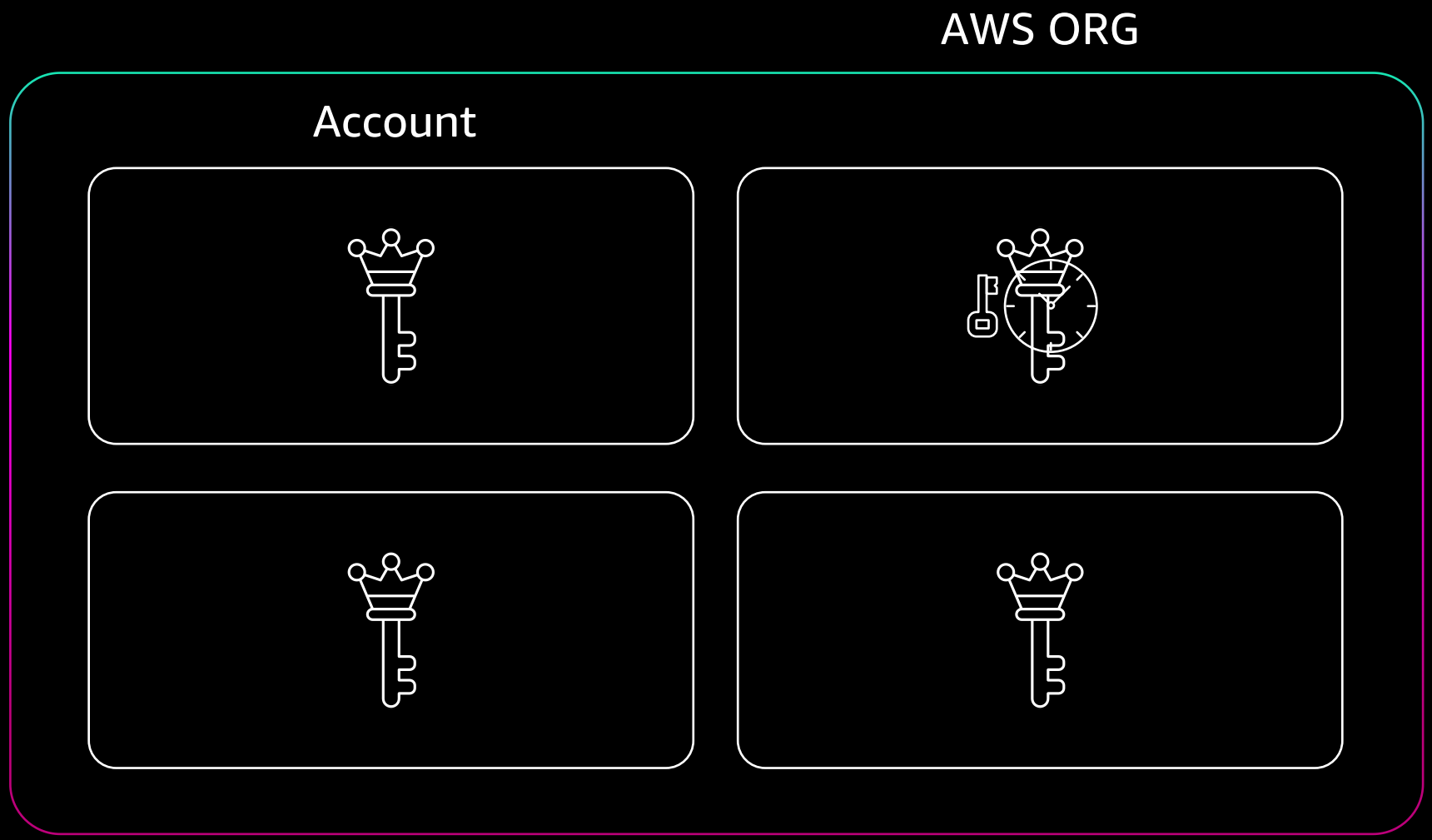
COP402: Dive Deep on AWS Cloud Governance

Monday, December 2nd
11:30 AM – 12:30 PM PST
Mandalay Bay

Centrally manage root access



Centrally manage root access



GENERALLY AVAILABLE

NEW

Centrally manage AWS IAM root access

for accounts in AWS Organizations

Remove unnecessary credentials

Simplify root access

Perform tightly-scoped, privileged tasks

LEARN MORE

SEC232: Secure by design: Enhancing the posture of root with central control

Wednesday, Dec 4th
8:30 AM – 9:30 PM PST
Mandalay

GENERALLY AVAILABLE

NEW

VPC Block Public Access

A new centralized declarative control that enables network and security administrators to authoritatively block Internet traffic for their VPCs

One-click, declarative control

Block Bi-directional or Ingress-only Internet connectivity via Internet Gateway

Add subnet exclusions for resources that requiring Internet access

Enforce settings at account or organization level

Integrated with Network Access Analyzer, VPC Flow Logs and Reachability Analyzer for advanced visibility

GENERALLY AVAILABLE 12/1

NEW

Declarative Policies

New organization policy that allows you to enforce desired configuration for an AWS service

- Easy to use – set up with a few clicks or commands
- Set once and Forget – once set configuration is maintained when new APIs and features are added
- Transparent – for end users through custom error messages

LEARN MORE

COP378: New governance capabilities for multi account environment

Tuesday, December 3rd
5:30 PM – 6:30 PM PST
Caesars Forum

GENERALLY AVAILABLE 12/1

NEW

Amazon GuardDuty Extended Threat Detection

AI/ML-powered multi-stage AWS threat detection

Rapid triage with auto-correlated attack sequence findings

Gain high-confidence insights from correlated disparate signals

Focus on the most critical threats and streamline response with MITRE ATT&CK® mappings and AWS-based remediation

LEARN MORE

SEC219: Uncovering sophisticated cloud threats with Amazon GuardDuty

Thursday, December 5th
11:00 AM – 12:00 PM PST
MGM Grand

aws

GENERALLY AVAILABLE 12/1

NEW

AWS Security Incident Response

Prepare for, respond to, and recover from security events

- Automate monitoring and investigation of security findings to free up your resources
- Accelerate communication and coordination for rapid incident response
- Access AWS security experts 24/7 for specialized assistance

LEARN MORE

SEC360: Respond and recover faster with AWS Security Incident Response

Wednesday, December 4th
12:00 PM – 1:00 PM PST
Mandalay Bay

GENERALLY AVAILABLE 12/1

NEW

Amazon OpenSearch Service Zero-ETL integration with Amazon Security Lake

Comprehensive visibility for security investigations and threat hunting

Faster time-to-security value with OCSF-based pre-built queries and dashboards

Optimize costs by querying data in place, indexing data on demand, and avoiding data duplication

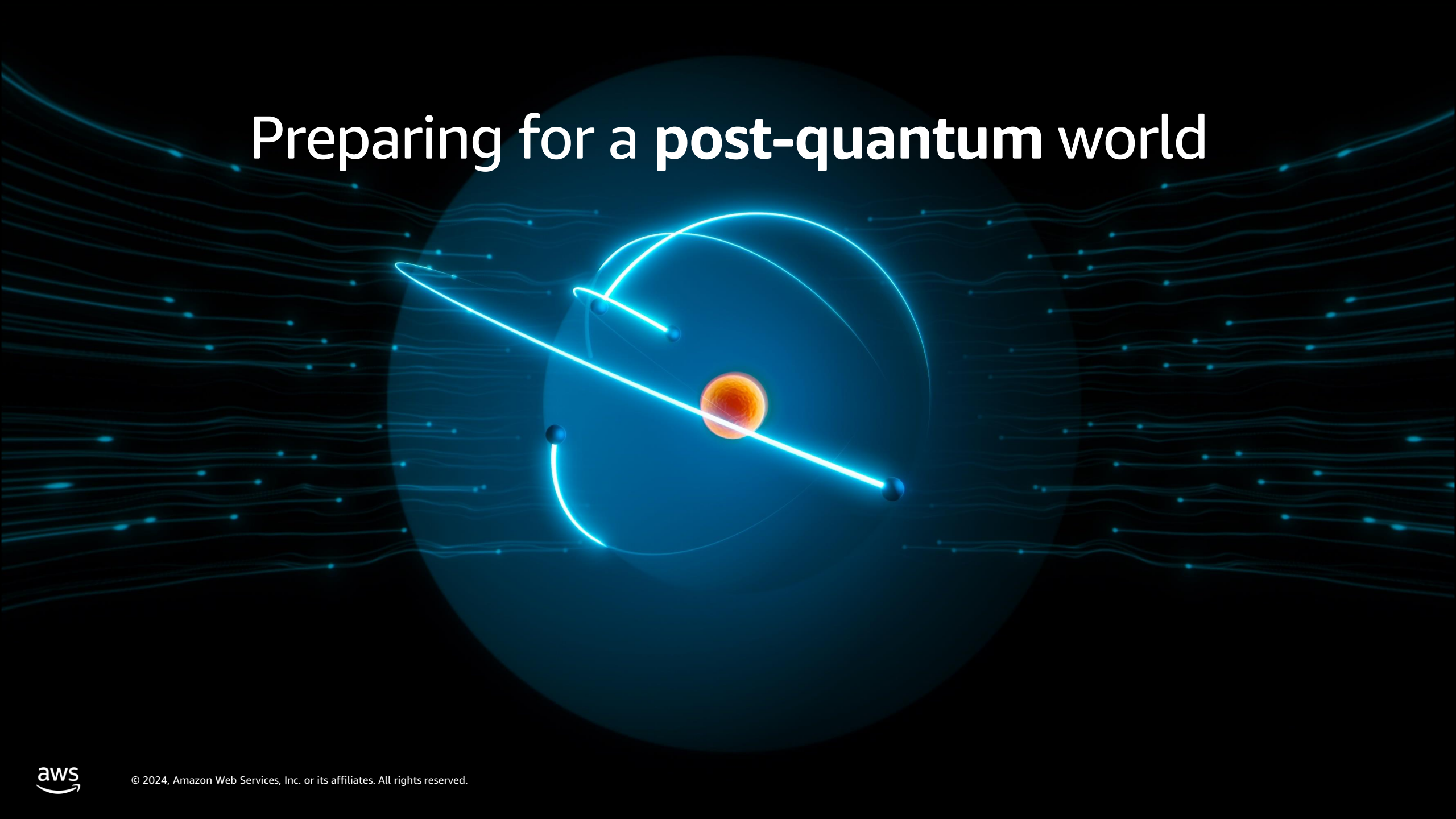
LEARN MORE

SEC321: Innovations in AWS detection and response

Wednesday, December 4th
10:00 AM – 11:00 AM PST
Mandalay Bay

Securing the **future**

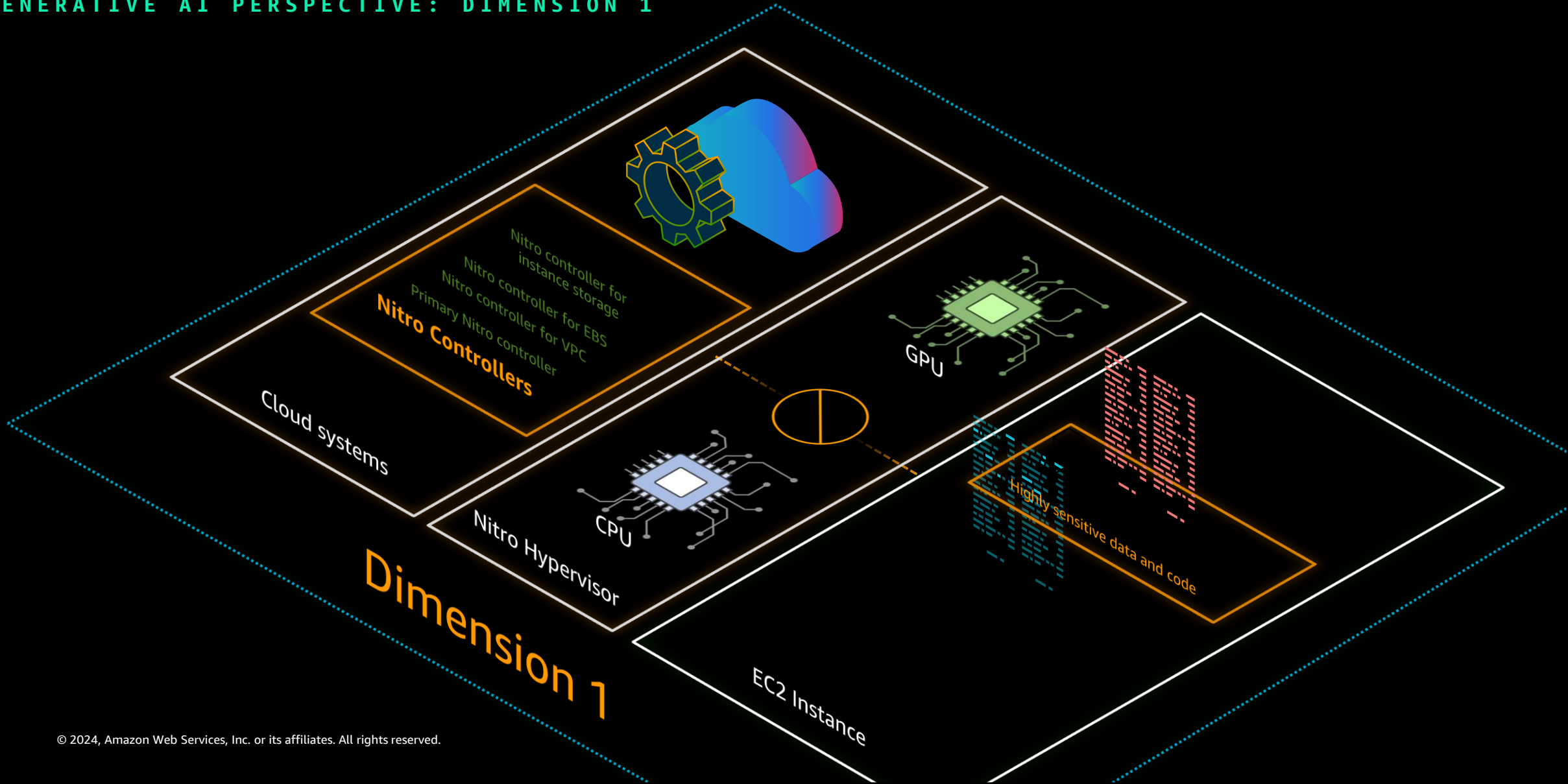
Preparing for a **post-quantum** world




Securing AI

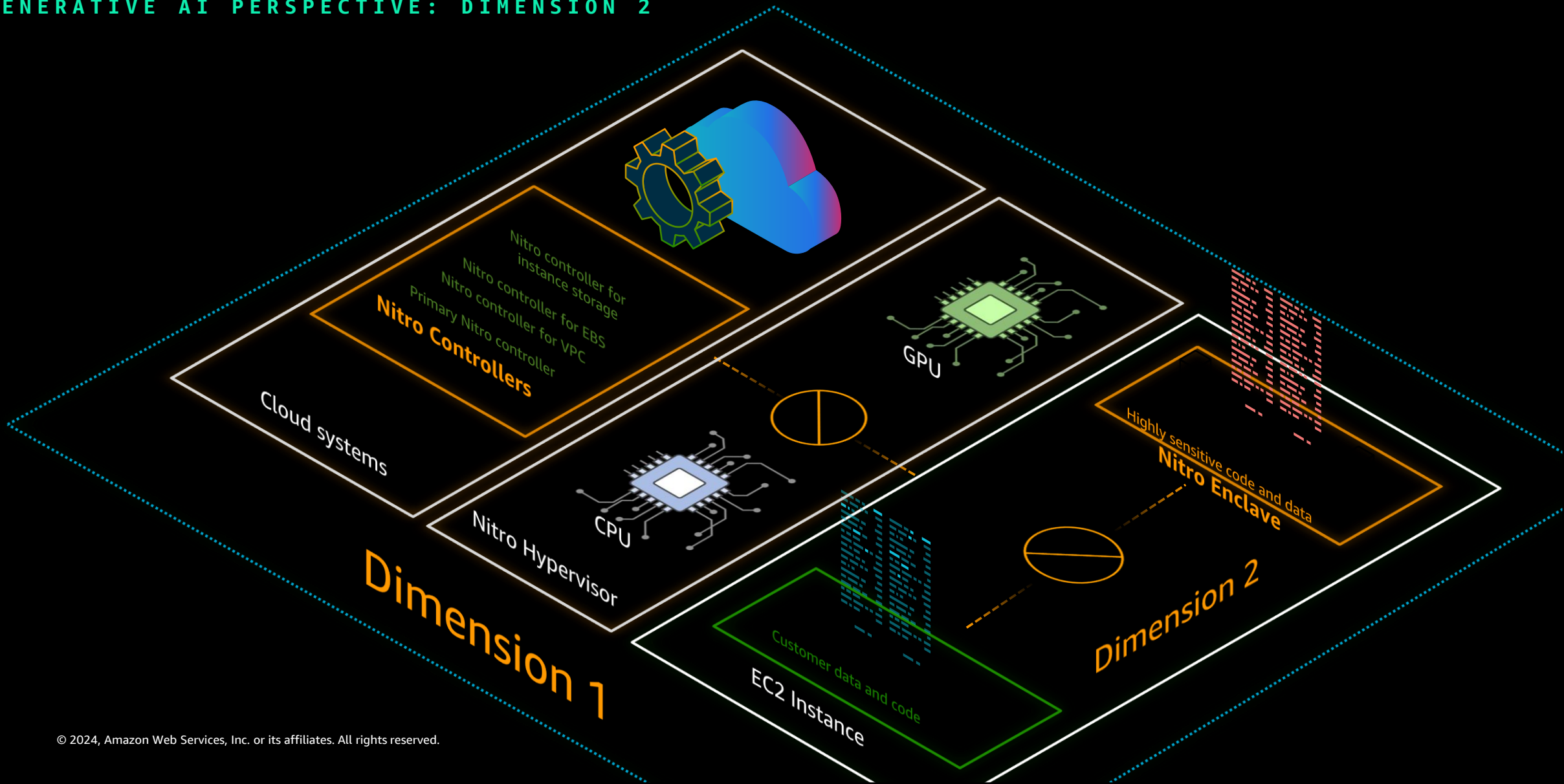
What is confidential computing?

A GENERATIVE AI PERSPECTIVE: DIMENSION 1



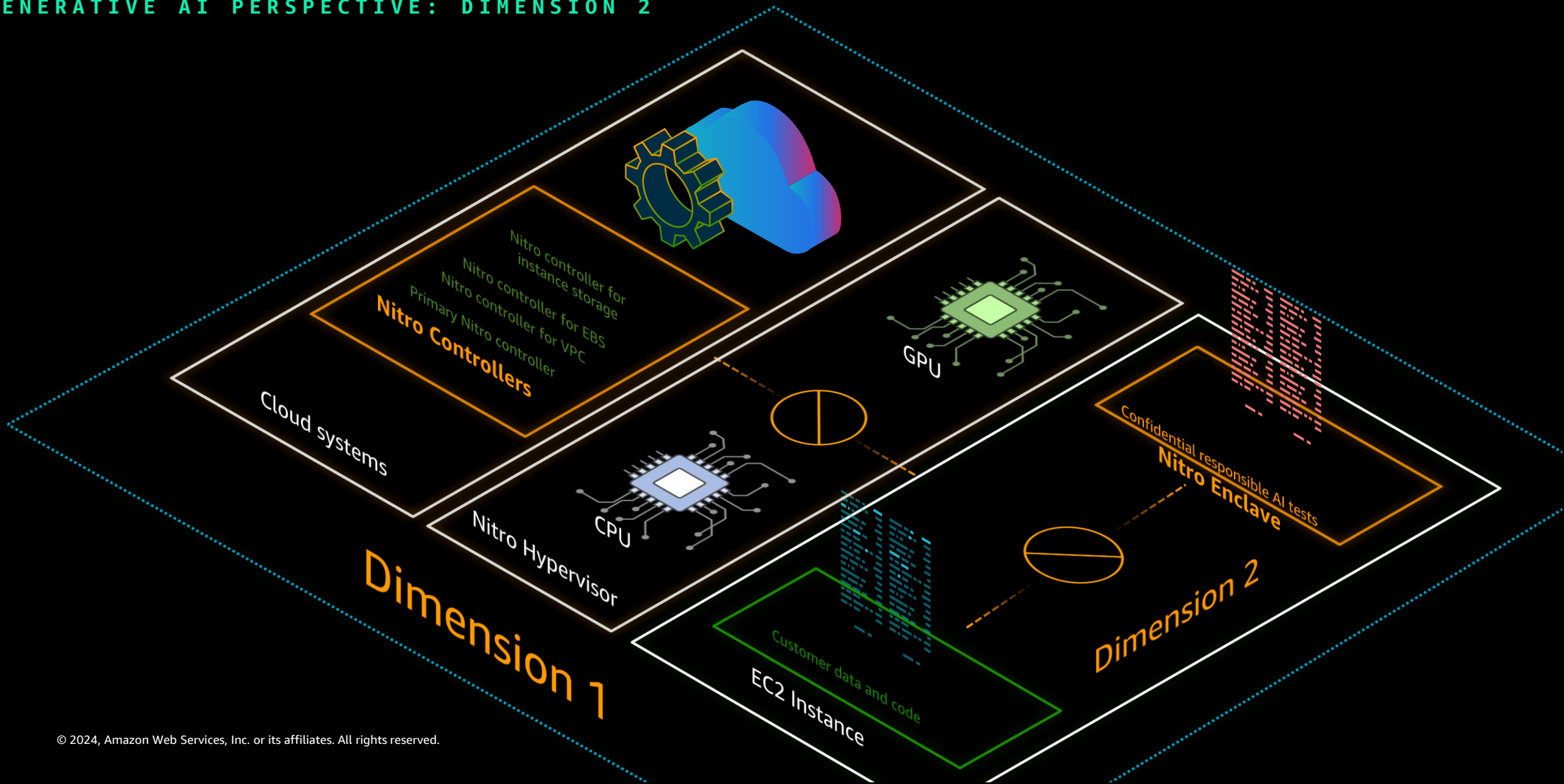
What is confidential computing?

A GENERATIVE AI PERSPECTIVE: DIMENSION 2



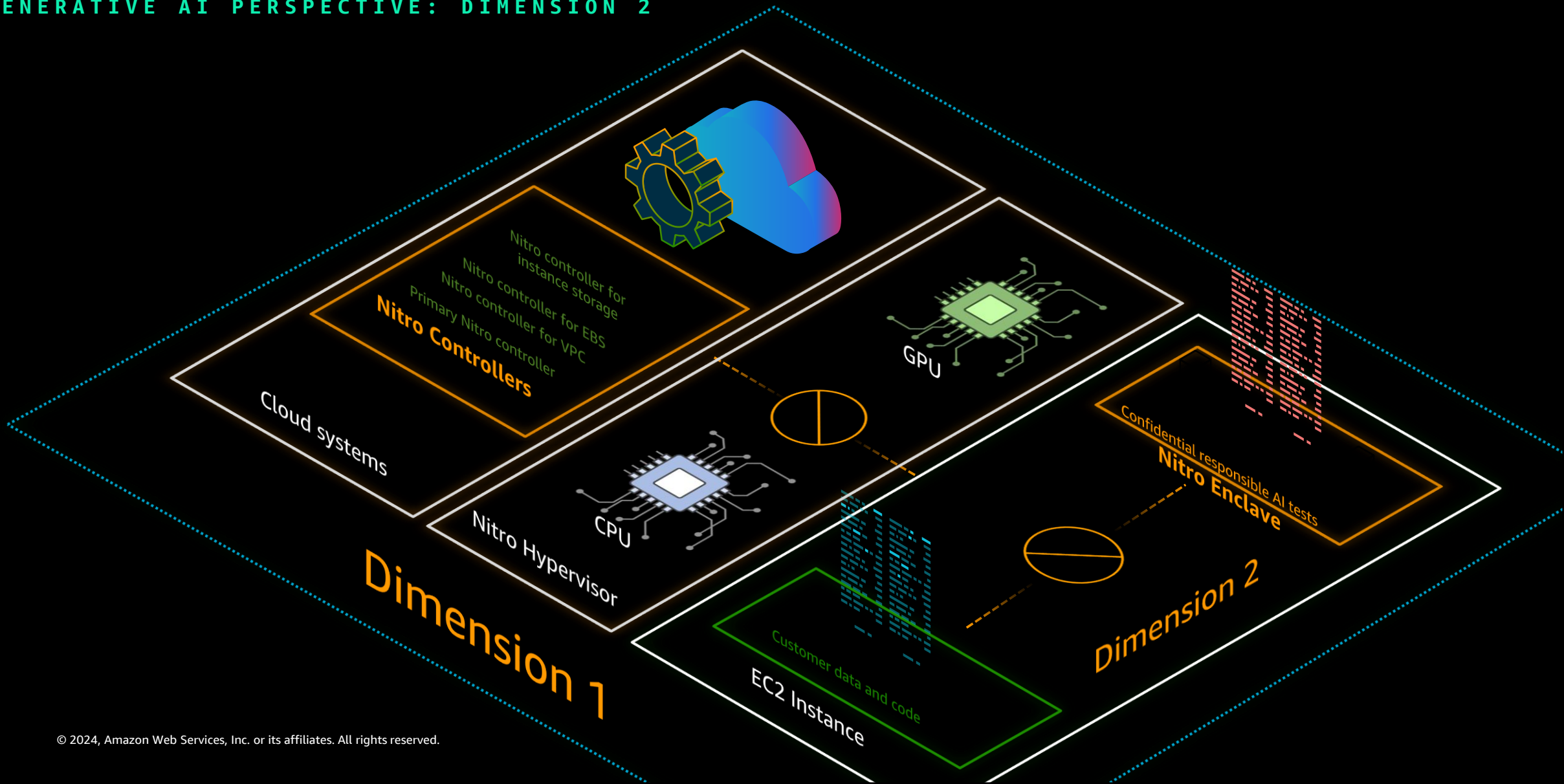
What is confidential AI testing?

A GENERATIVE AI PERSPECTIVE: DIMENSION 2



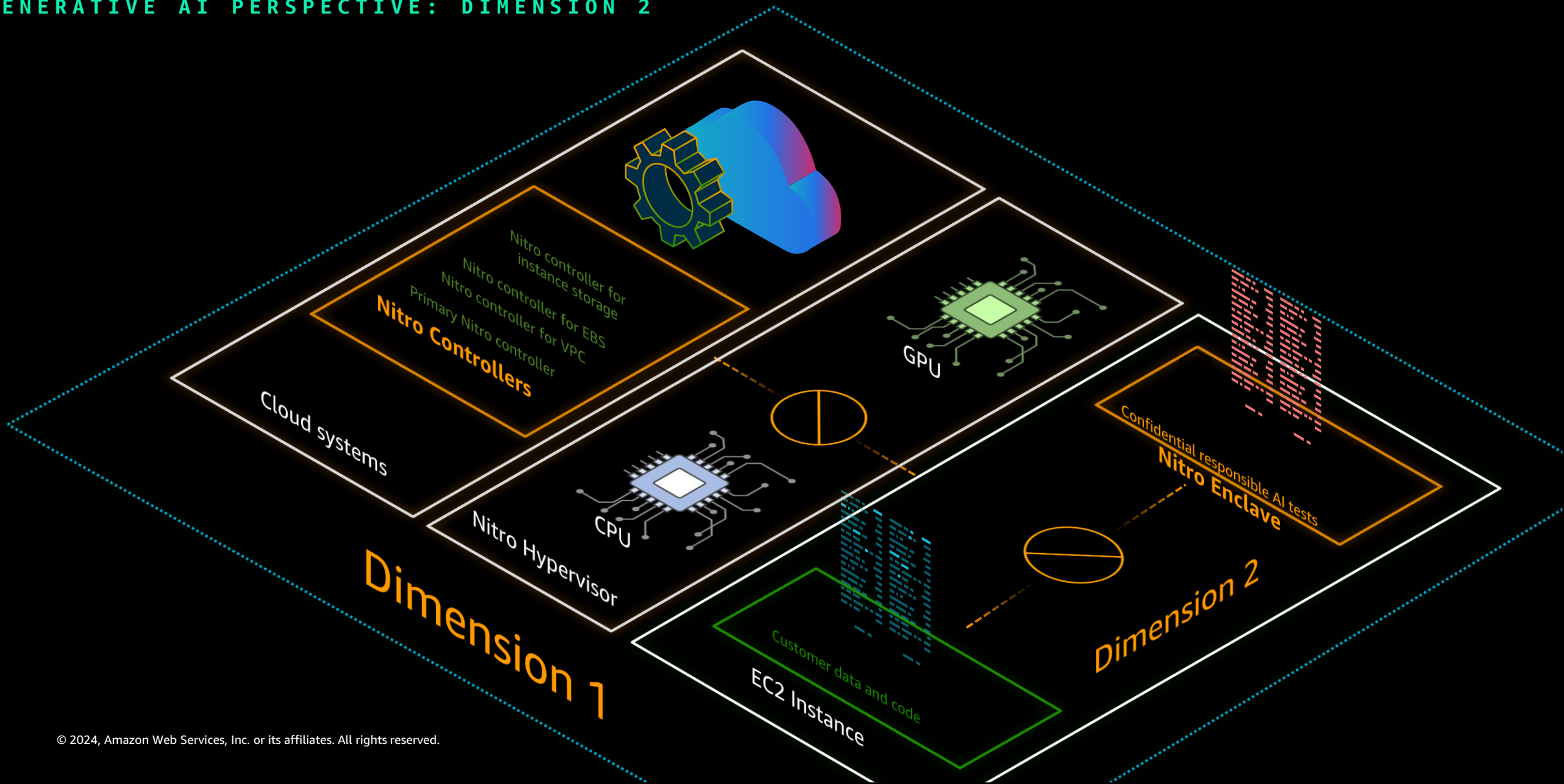
What is confidential AI testing?

A GENERATIVE AI PERSPECTIVE: DIMENSION 2

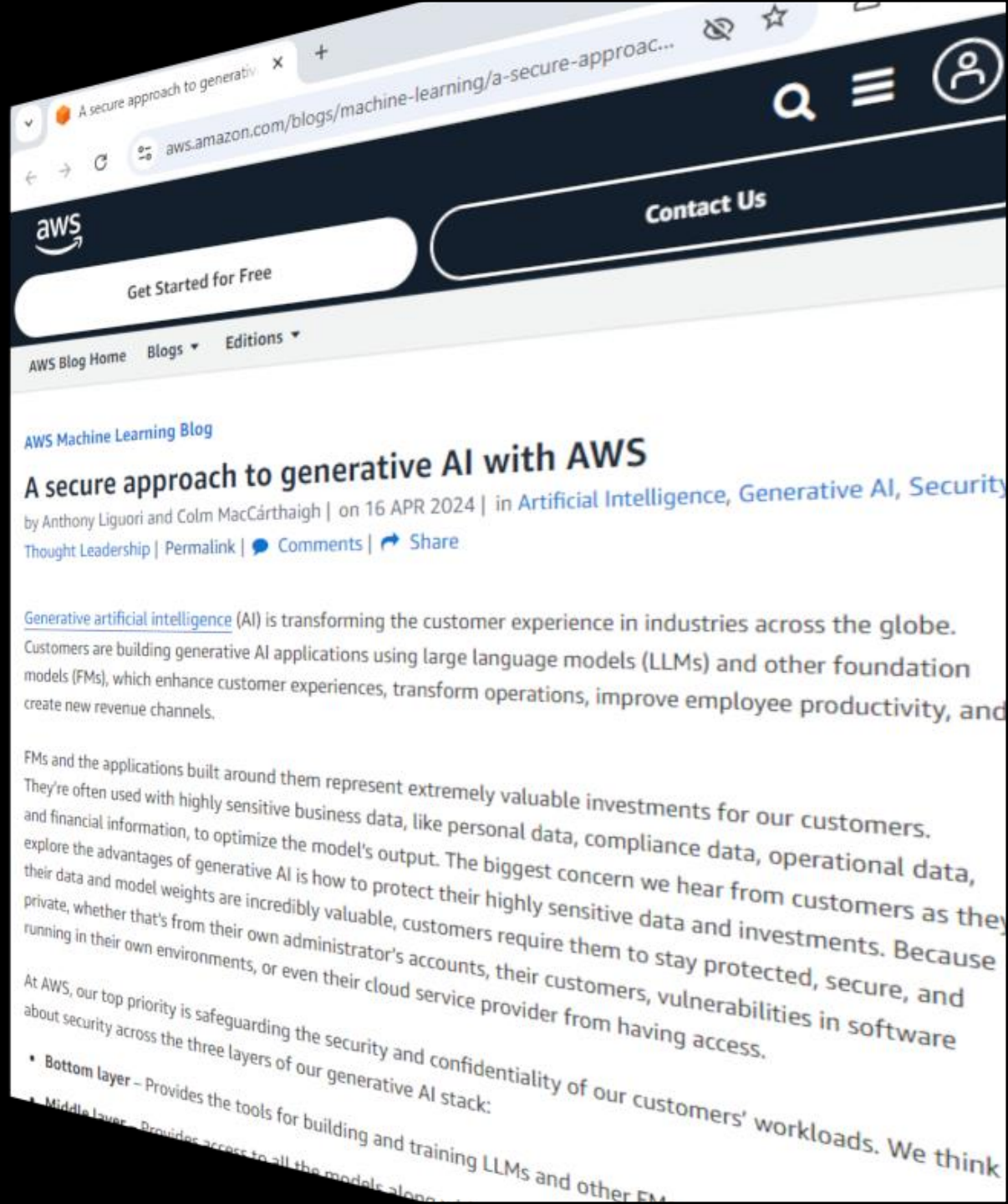


What is confidential AI testing?

A GENERATIVE AI PERSPECTIVE: DIMENSION 2



What about confidential AI computing?



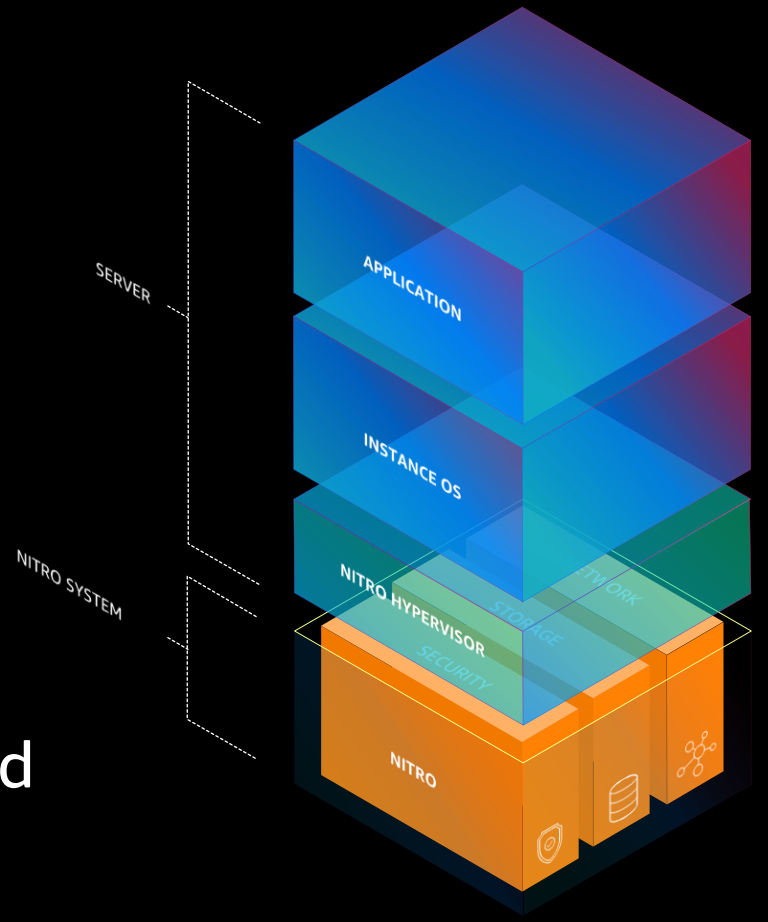
Extending the Nitro System's end-to-end protection to **ML accelerators**

Encrypt sensitive AI data using keys you own and control

Store that data in a location of your choice

Securely transfer data to an isolated compute environment for inferencing

Planned for the upcoming NVIDIA GB200 NVL72 and Trainium2



Jason Clinton

Chief Information Security Officer, Anthropic


aws

Upgraded Claude 3.5 Sonnet

NEW

+ AWS strikes the ideal balance: market-leading intelligence, speed, and cost

Use cases

- Code generation
- Advanced chatbots
- Knowledge Q&A
- Visual data extraction
- Robotic process automation (RPA)
- Computer use (public beta)

Anthropic's most intelligent model yet

	Claude 3.5 Sonnet (upgraded)	Claude 3.5 Sonnet	GPT-4o	Gemini 1.5 Pro
Graduate level reasoning *GPQA (Diamond)*	65.0% 0-shot CoT	59.4% 0-shot CoT	53.6% 0-shot CoT	59.1% 0-shot CoT
Undergraduate level knowledge *MMLU Pro*	78.0% 0-shot CoT	75.1% 0-shot CoT	—	75.8% 0-shot CoT
Agentic coding *SWE-bench Verified*	49.0%	33.4%	—	—
Code *HumanEval*	93.7% 0-shot	92.0% 0-shot	90.2% 0-shot	—
Math problem-solving *MATH*	78.3% 0-shot CoT	71.1% 0-shot CoT	76.6% 0-shot CoT	86.5% 4-shot CoT
Multilingual math *MGSM*	92.5% 0-shot CoT	91.6% 0-shot CoT	90.5% 0-shot CoT	—
Reasoning over text *DROP, F1 Score*	88.3 3-shot	87.1 3-shot	83.4 3-shot	—
Agentic tool use *TAU-bench*	Retail 69.2% Airline 46.0%	Retail 62.6% Airline 36.0%	—	—

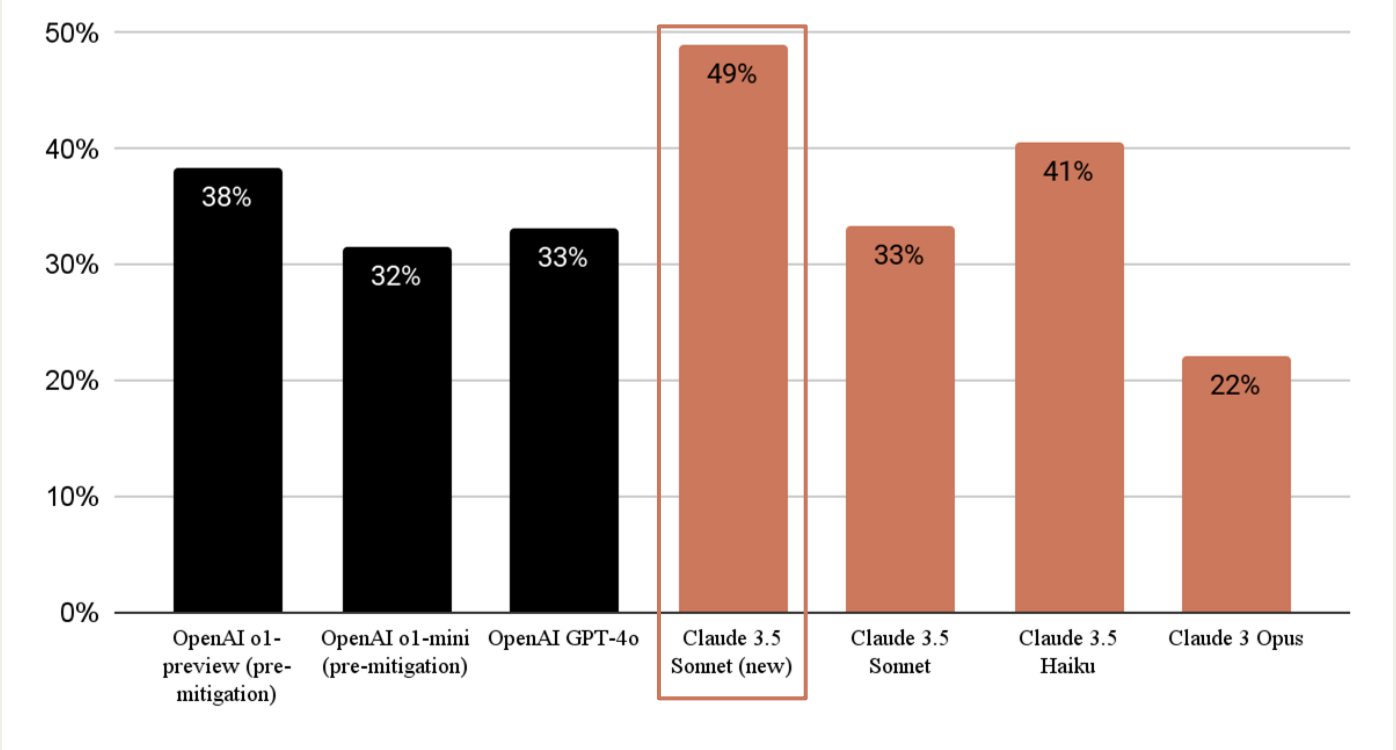
ANTHROP\C

Claude 3.5 Sonnet is leading the coding revolution

while also being significantly faster and cheaper than other models

SWE-bench Verified

Assesses a model's ability to complete real-world software engineering tasks and understand, modify, and test code with tools



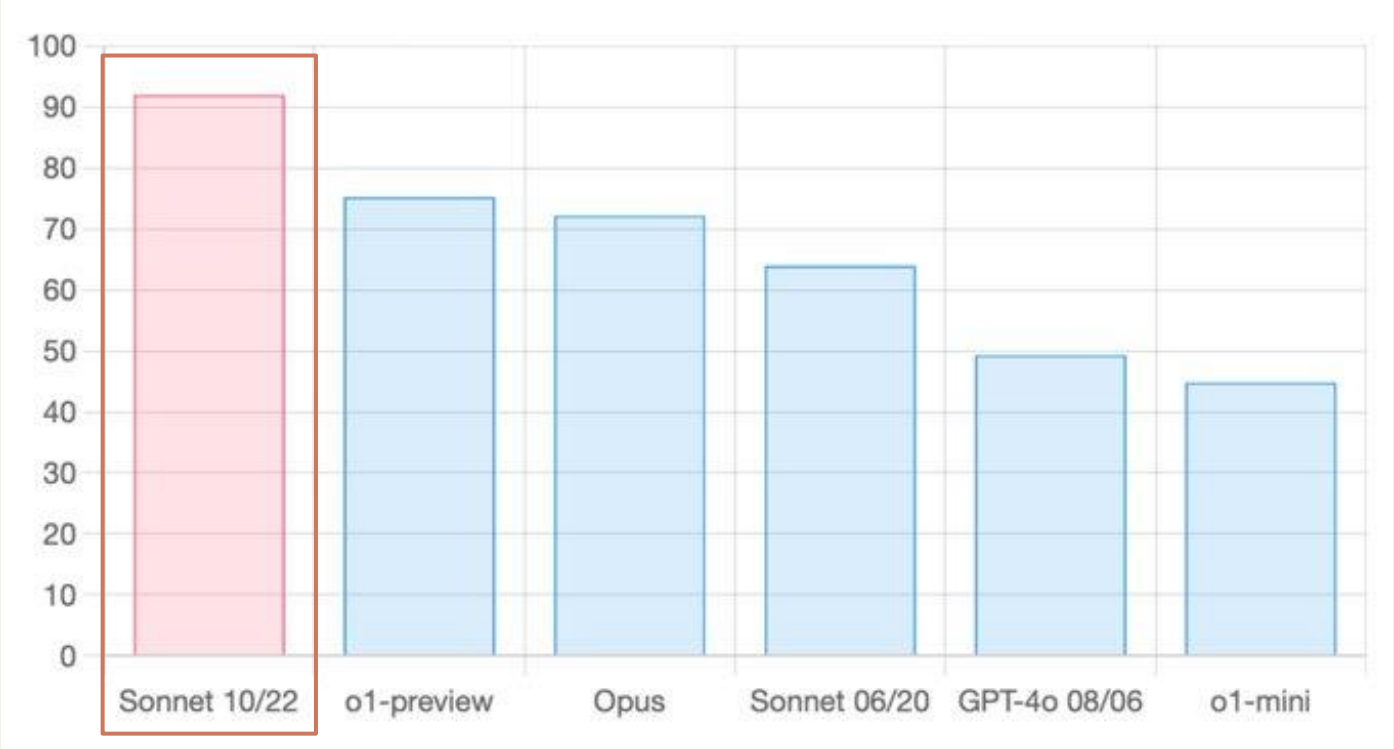
Sources: OpenAI o1 model system card, Anthropic model card (October 2024 3.5 model addendum)

Claude 3.5 Sonnet is leading the coding revolution

despite being significantly faster and cheaper than other models

Aider's refactoring benchmark

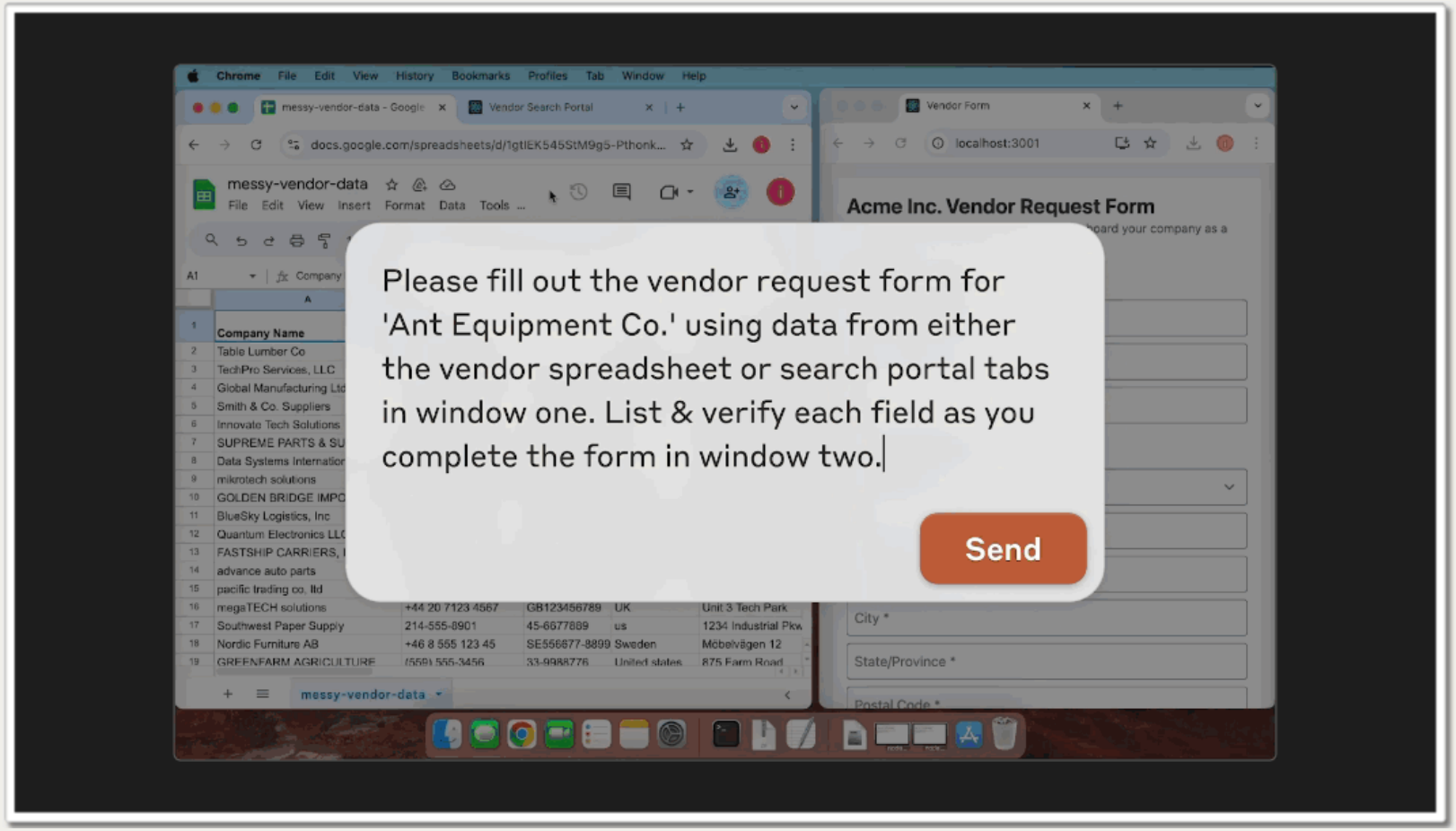
A more challenging benchmark which tests the model's ability to output long chunks of code without skipping sections or making mistakes

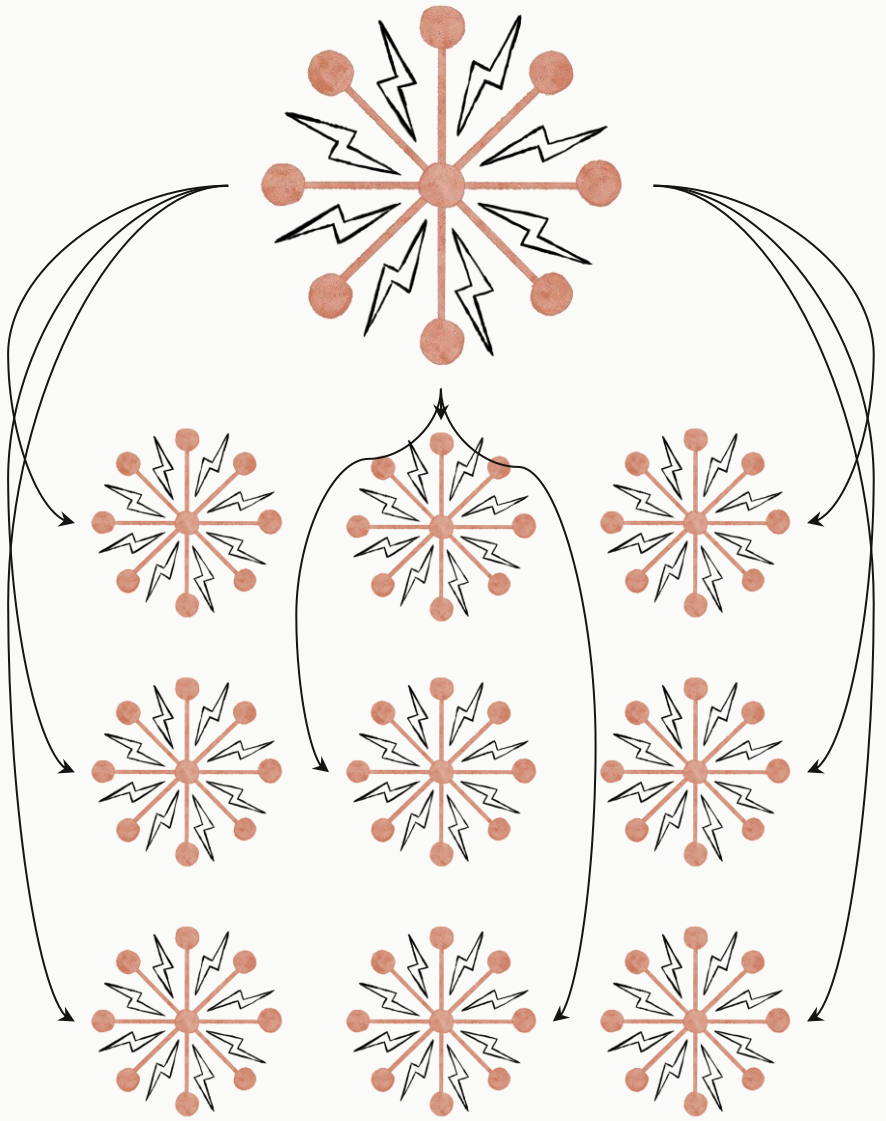


Sources: Aider LLM Leaderboards

Computer Use

Computer use is Claude's ability to **perform tasks by interpreting screenshots and automatically generating the necessary computer commands**





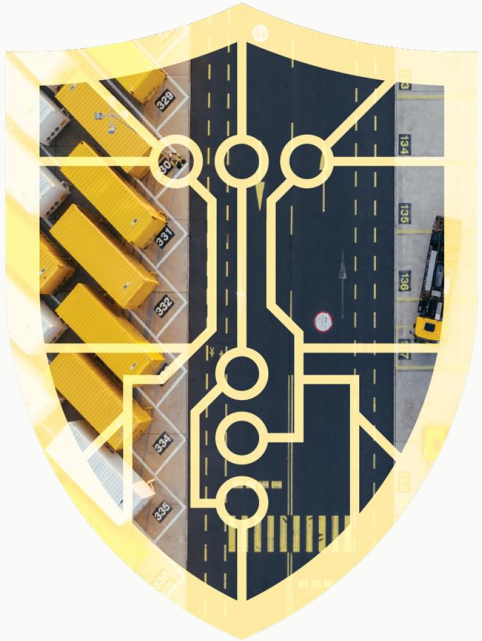
Subagent automation

What's next

Cybersecurity implications

Vulnerability discovery

- We think that in the next 3-15 months: a great incremental increase in defensive and offensive utilization
- The is dual-use: we can prevent shipping bugs and find the existing ones, but also…

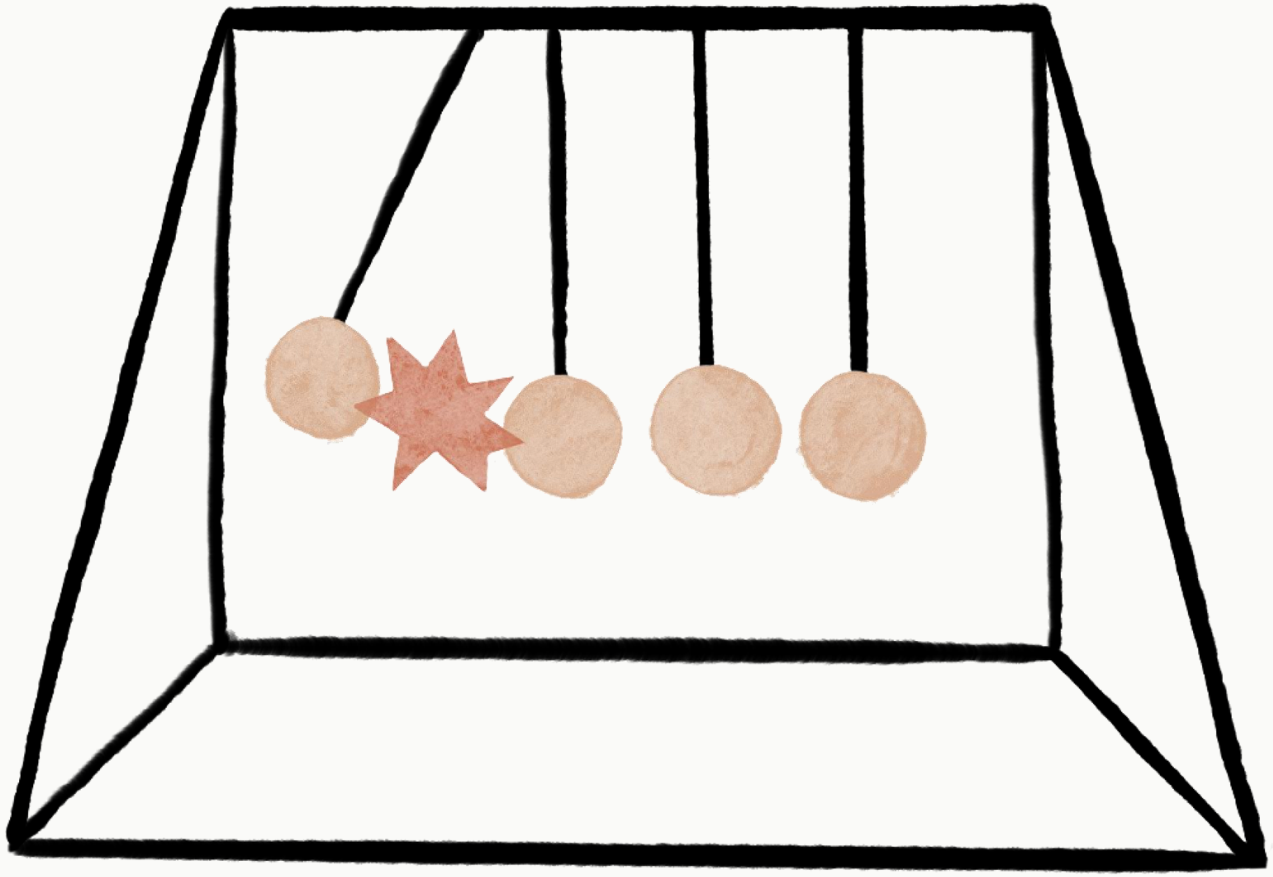


AIxCC

AI CYBER CHALLENGE

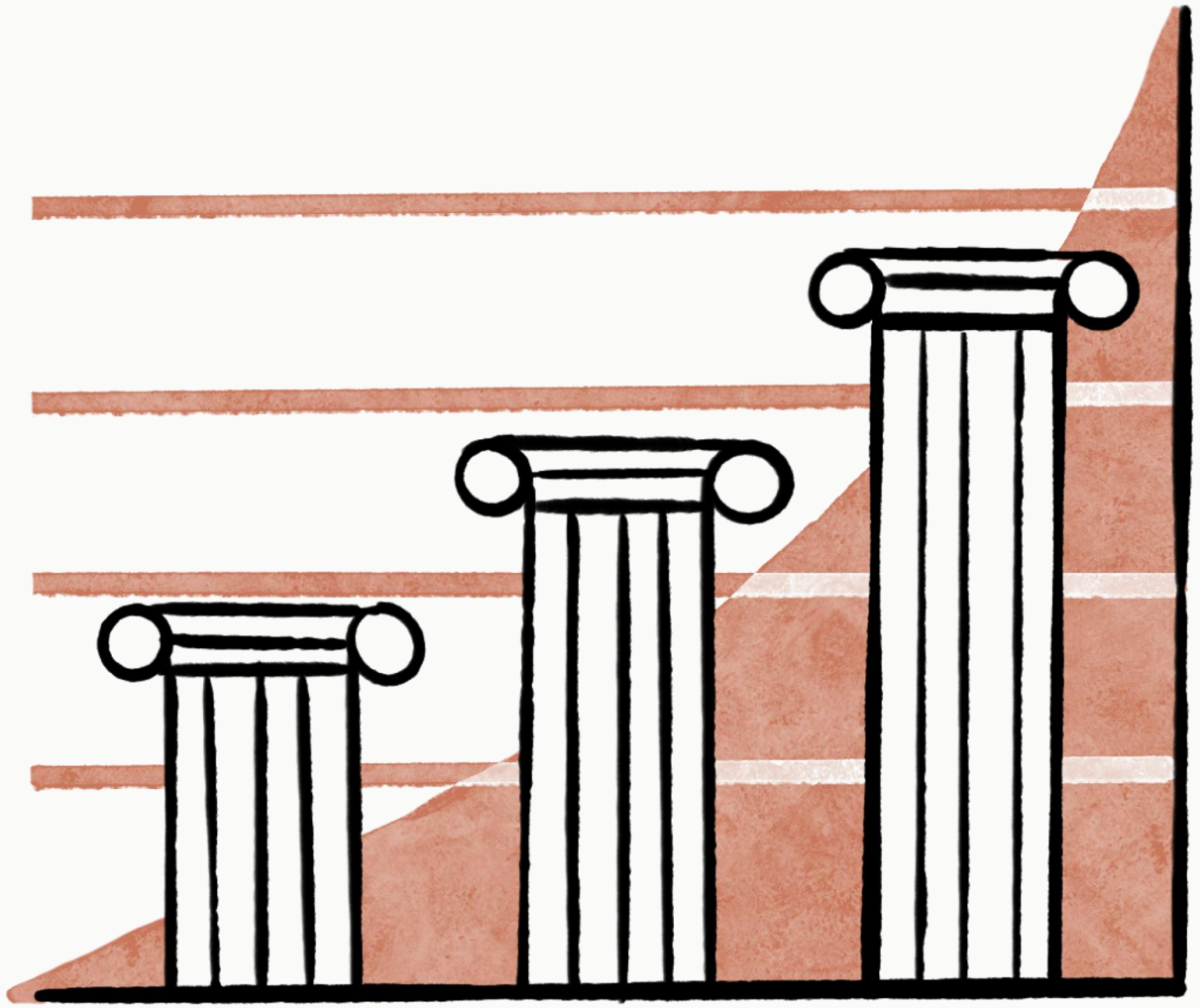
AI access to data and identity

- Unprecedented, unbounded access to corporate systems and enterprise data
- Unclear where human stops and AI access begins



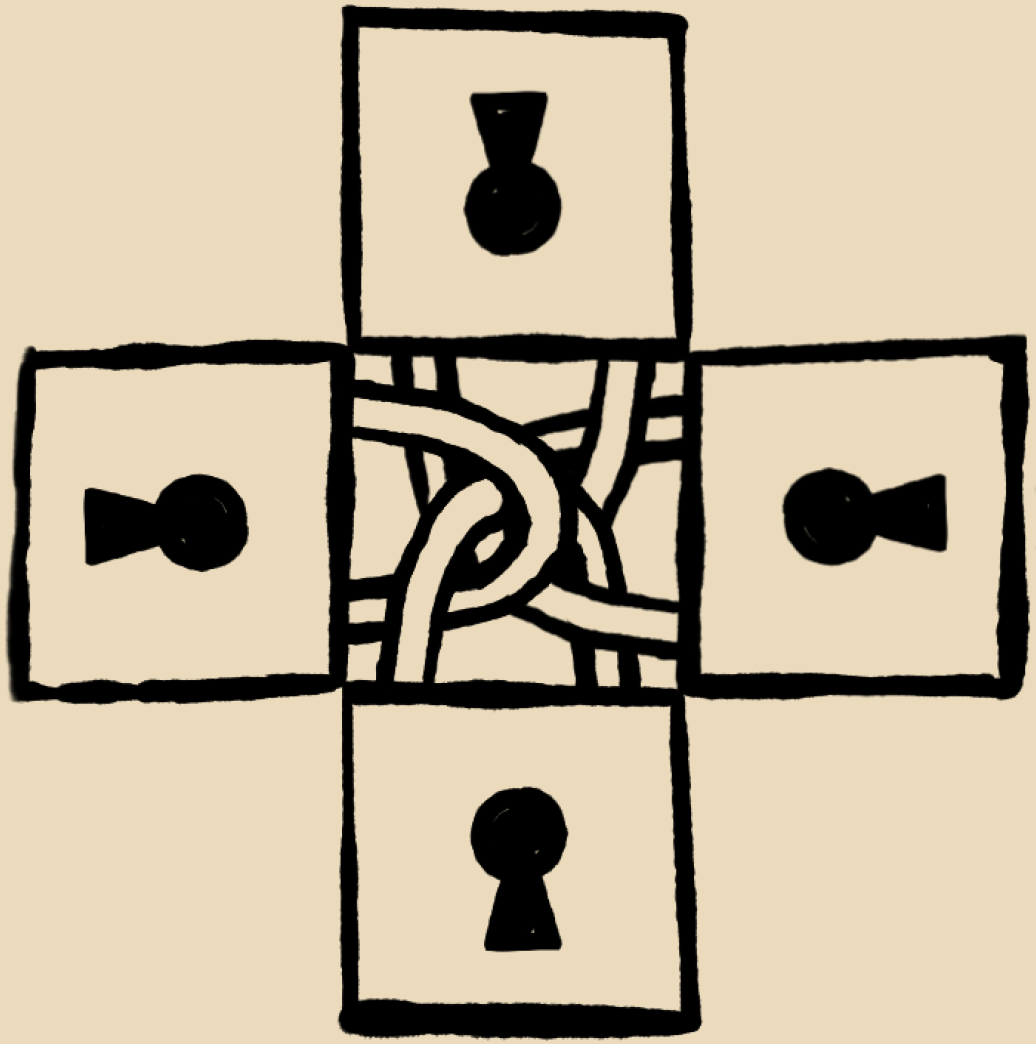
Responsible Scaling Policy

- RSP introduces ASL framework: tiered safety protocols for AI development
- Currently at ASL-2, with stricter controls planned for higher-risk levels
- Framework is iterative, collaborative, and supports broader regulation

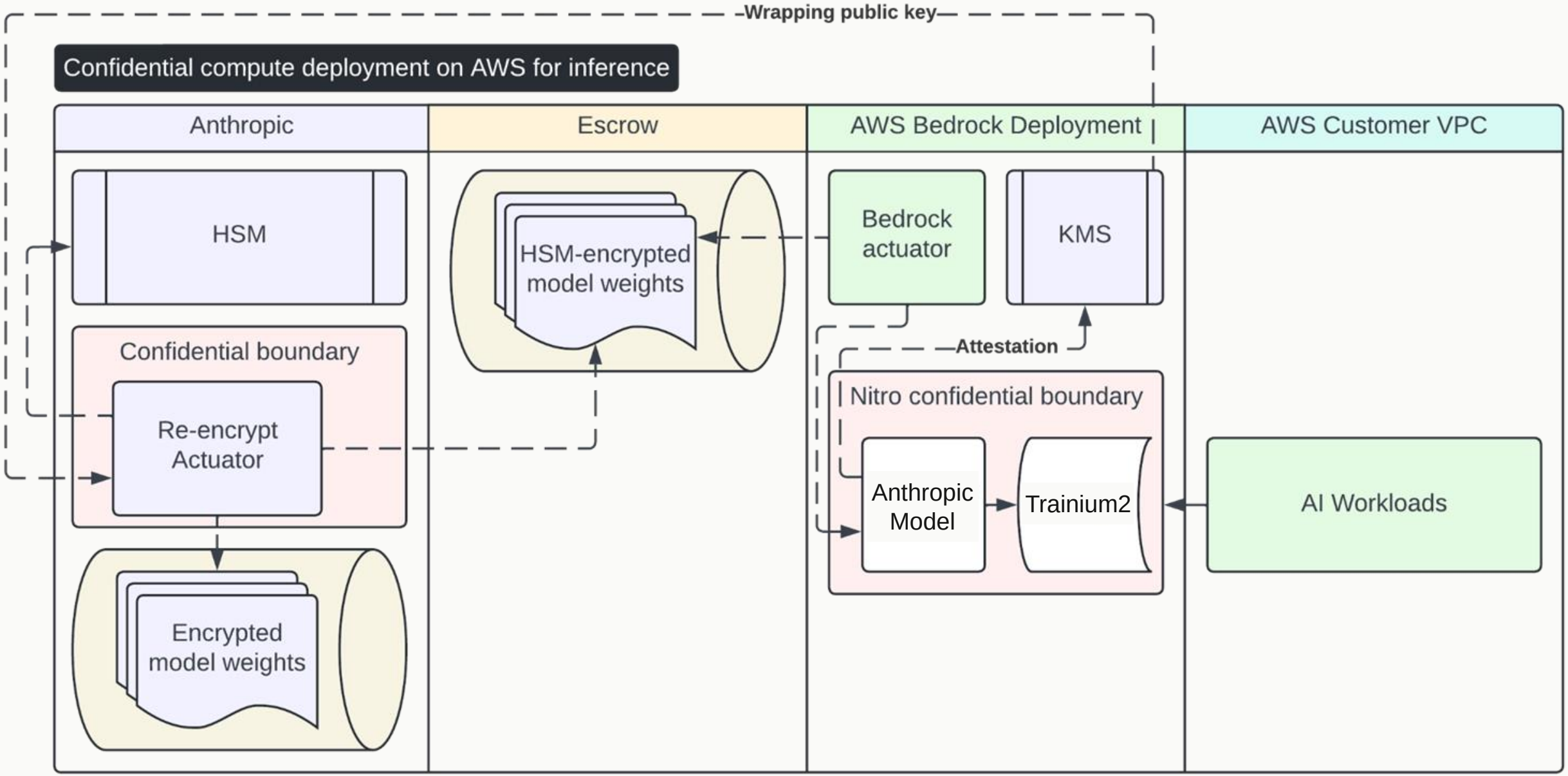


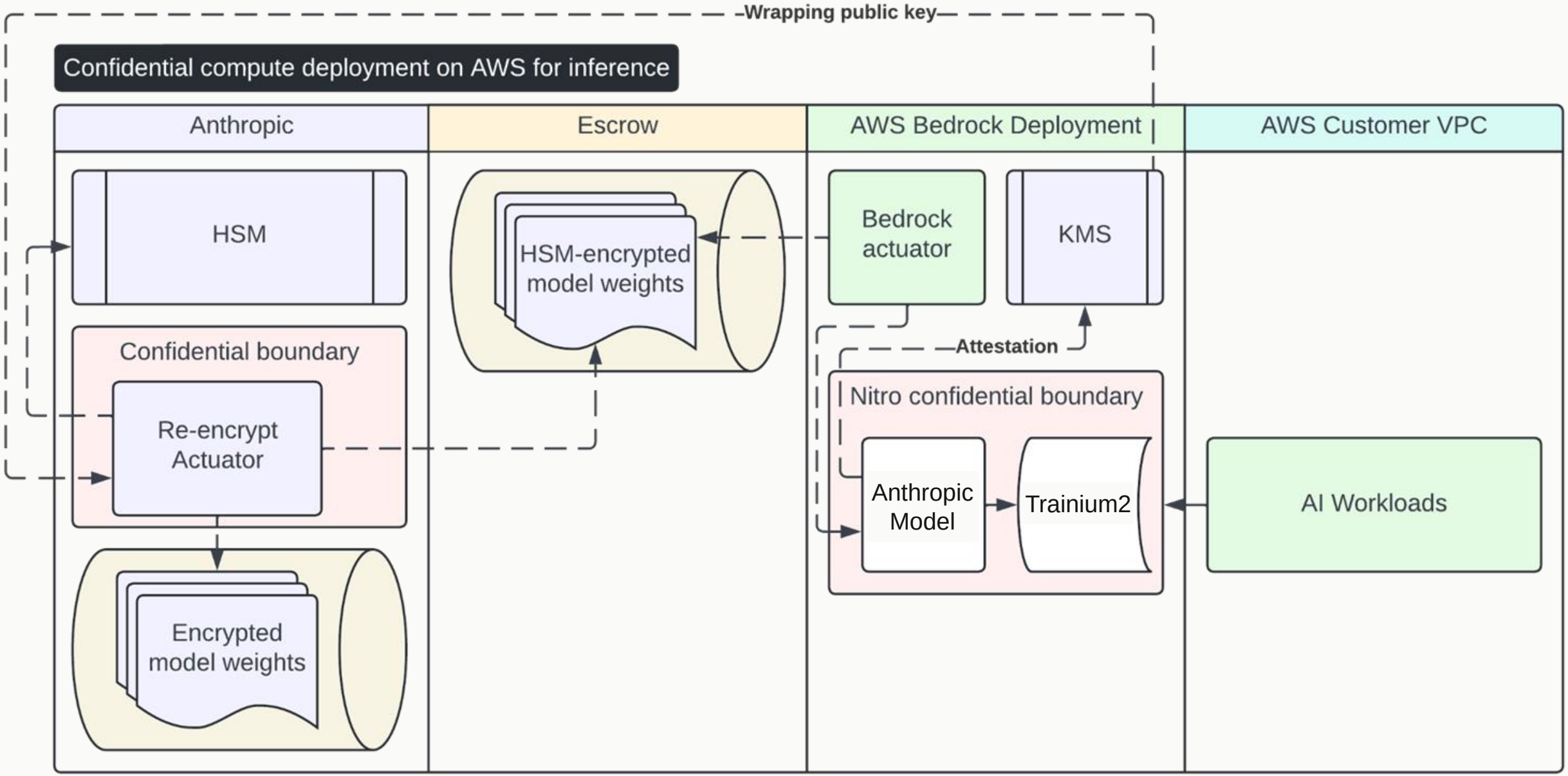
The path to ASL-4

Confidential deployment



ANTHROP\C


Wrapping public key
Confidential compute deployment on AWS for inference
Anthropic
Escrow
AWS Bedrock Deployment
AWS Customer VPC
HSM
HSM-encrypted model weights
Bedrock actuator
KMS
Confidential boundary
Re-encrypt Actuator
Attestation
Nitro confidential boundary
Anthropic Model
Trainium2
AI Workloads
Encrypted model weights


Wrapping public key
Confidential compute deployment on AWS for inference
Anthropic
Escrow
AWS Bedrock Deployment
AWS Customer VPC
HSM
HSM-encrypted model weights
Bedrock actuator
KMS
Confidential boundary
Re-encrypt Actuator
Attestation
Nitro confidential boundary
Anthropic Model
Trainium2
AI Workloads
Encrypted model weights

Chris Betz

Chief Information Security Officer, AWS

YOUR TURN

Raise your **security bar**

Consider a **security champions program** in your own team

Build a data perimeter with **Resource Control Policies**

Block public Internet access for **VPC resources**

Standardize resource configurations with **Declarative Policies**

Related sessions

- SEG103 — Shaping culture: Mental models and mechanisms
- SEC217 — Building a resilient and effective culture of security
- SEC218 — Emotionally intelligent security leadership to drive business impact
- SEC219 — Uncovering sophisticated cloud threats with Amazon GuardDuty
- SEC232 — Secure by design: Enhancing the posture of root with central control
- SEC321 — Innovations in AWS detection and response
- SEC342 — Secure by design: Enhancing the posture of root with central control
- SEC360 — Respond and recover faster with AWS Security Incident Response
- SEC361 — How AWS scales active defense
- SEC403 — Generative AI for security in the real world
- COP378 — New governance capabilities for multi account environment
- COP402 — Dive Deep on AWS Cloud Governance

Save the date for AWS re:Inforce

JUNE 16 - 18, 2025 | PHILADELPHIA, PA

AWS re:Inforce

Thank you!

Please complete the session survey in the mobile app

Chris Betz
Chief Information Security Officer, AWS
linkedin.com/in/chris-betz-903b739b/

Becky Weiss
VP and Distinguished Engineer, AWS
linkedin.com/in/becky-weiss/

Rodrigo Castillo
CTO, Commonwealth Bank of Australia
linkedin.com/in/rodrigocastilloof

Jason Clinton
Chief Information Security Officer, Anthropic
linkedin.com/in/jason-d-clinton/