

Hairpin Edge Demo

Edge-Local Mission Data Processing on AWS

Eliminating the “hairpin” round-trip with edge-local compute, at-source data reduction, and Zero Trust data protection.

Scale AI (Lux) + XQ + AWS

U.S. Space Force / PWSA tactical edge · GovCloud IL5 / Secret IL6 · Compute-led framing

The Hairpin Round-Trip

Today, mission data is collected at the orbital or tactical edge, downlinked to a centralized ground data center for processing, then pushed back out to the warfighter.

That round-trip — the “hairpin” — adds a distance-induced latency penalty and depends on a downlink that is a hard physical bottleneck. In contested (DDIL) conditions the reach-back link is the first thing to fail, turning a connected capability into a liability.

Net effect: time-critical intelligence arrives too late to act on.

~2%

of recorded satellite data reaches the ground

5–10 min

ground-station contact window per pass

~12 GB

typical usable data per pass

0.1–2 Gbps

legacy RF downlink vs. 10–100 Gbps optical

Compute at the Collection Point

Remove the round-trip by processing where data is collected — then downlink only distilled insight, secure the residual, and sync opportunistically.

1

Edge-local compute for Native AI/ML

AI/ML operating on forward-deployed hardware without requiring a cloud connection to "think" or correlate threats .

2

Zero Trust data protection

Security policies that are cryptographically bound to the data payload itself, proving that access control is enforced locally, regardless of the transport network.

3

Mission Survivability

DDIL and disadvantaged edge user support, seamless automated failover from classified military networks (MILSAT) to commercial SATCOM transport without risking data spillage or violating compliance.

4

At-Source Data Reduction

Demonstrate that LUX reduces raw sensor data 10–50x at the collection point through classification and feature extraction—transmitting coordinates and decisions, not raw imagery. This architecture breaks the LEO downlink bottleneck by sending only decision-ready products over the constrained link to Scale Donovan processing through Bedrock.

Scale AI (Lux) — What We Deliver

The agentic runtime that executes the mission decision loop at the collection point — turning raw feeds into decisions, on-node, in mission time.

Lux agent runtime

Scale AI Lux orchestrates multi-agent workflows, retrieves knowledge locally, and correlates data in real time directly at the point of collection—meaning you don't need a connection back to the cloud

Mission-specific reduction model

A detection / classification (and imagery-compression) model built into the Lux pipeline as a pilot deliverable — the piece that shrinks the downlink and raises usable data per pass.

Space Domain Awareness

SDA relies on a highly fragmented network of radar, optical, infrared, and radio-frequency sensors across the globe. LUX™ acts as a "single pane of glass" data-fusion engine, pulling disparate sensor inputs into a unified operational picture. It translates raw, raw-signal telemetry into real-time indications and warnings.

Platform classified **authorizations**

Scale's Donovan runs today in accredited classified networks (SC2S, SIPR+, JWICS) — evidence of disconnected, accredited operation at IL5/IL6-equivalent levels, not just capability on paper Scale Government Platform (SGP) carries FedRAMP High, SOC 2 Type II, and ISO 27001 — platform-level trust the pilot inherits as it deploys into GovCloud (IL5) and Secret Cloud (IL6).

XQ — What We Deliver

Data-centric Zero Trust that protects and governs each object from the point of creation — the patented commercial solution AWS selected for its U.S. Government Zero Trust Data pillar.

XQ Mission Outcomes & Key Benefits

- **Data-Centric Zero Trust Security & Granular Control:**
 - **Benefit:** Protection and governance are attached to each individual data object from the moment of creation. Features like the **XQ DataBase Proxy** (row-level encryption) and **XQ File Vault** ensure security follows the file across Amazon S3/EC2 or local nodes.
 - **Mission Outcome:** Secure, fine-grained access control is maintained across edge nodes, VPCs, and cloud boundaries without needing application changes or compromising security compliance (meeting U.S. Government Zero Trust Data pillar standards).
- **Chain of Custody & Administrative Separation:**
 - **Benefit:** The **XQ Platform** separates administrative controls from KMS/IAM and maintains an auditable chain of custody per data object.
 - **Mission Outcome:** Multi-tenant or coalition environments can share critical mission data safely with verified accountability, preventing unauthorized access or data tampering.

XQ Platform components

XQ Platform: containerized policy, data detection, validation & key server + management portal (on-prem or AWS). Separates Admin from KMS/IAM; chain of custody per data object.

XQ Secure Edge: encrypts & governs data at the point of creation, before it enters the network — edge to cloud.

XQ DataBase Proxy: row-level encryption & access control before data reaches the database, no app changes.

XQ Server / Client File Vault: encryption & access that follow the file; mounts Amazon S3 / EC2.

XQ Gateway: encryption, policy enforcement & user access for the application VPC.

DoD Zero Trust — Data pillar fit

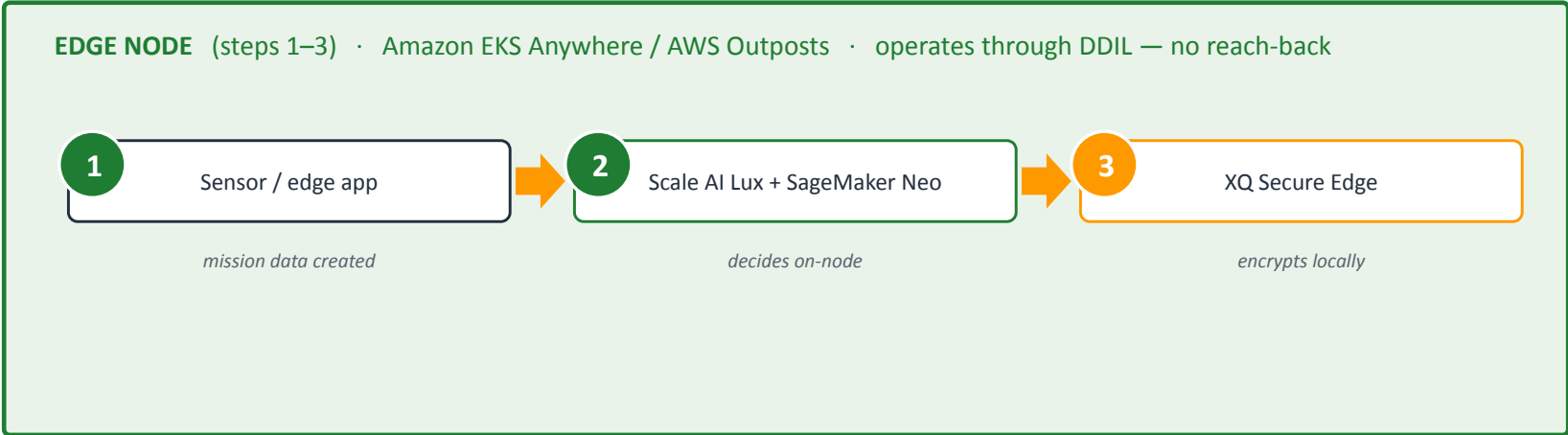
Maps to all seven components of the DoD Zero Trust Data pillar as the only patented, commercially available solution:

- Enterprise data governance
- Data catalog risk alignment
- Data labeling & tagging
- Data access control (RBAC, geo, time)
- Data monitoring & sensing
- Data loss prevention
- Data encryption & rights management

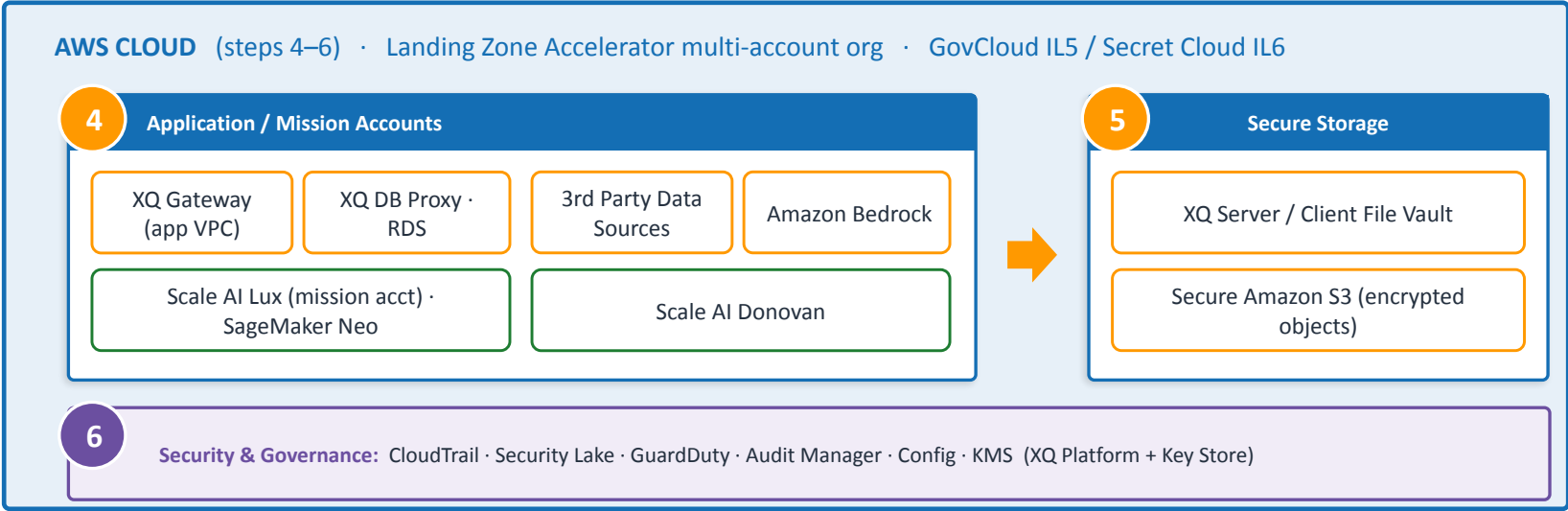
Compliance: CMMC L2, NIST 800-171, CISA, FISMA, ITAR — deploy in ~a week, not a year.

Hairpin Edge Solution on the AWS Landing Zone Accelerator (IL5 / IL6)

● Scale AI (Lux) — edge compute ● XQ — Zero Trust data ● AWS account / VPC ● Security & governance



Downlink via AWS Ground Station → only distilled, encrypted results cross into the cloud



How the vendors work together

AT THE EDGE

- 1 Data created at the edge**
A sensor / edge app generates mission data at the collection point.
- 2 Scale AI Lux decides on-node**
Lux runs the decision loop locally (EKS Anywhere / Outposts) on a Neo-compiled model — no round-trip.
- 3 XQ Secure Edge protects it**
An ephemeral, policy-bound key encrypts the result locally before anything leaves the node.

IN THE AWS CLOUD

- 4 Scale Insight + XQ governance in the cloud**
XQ Gateway + DB Proxy enforce row-level access in the mission accounts; nothing decrypts without a real-time policy match.
- 5 XQ File Vault stores it**
Encrypted results land in Secure S3 via XQ File Vault — protection follows the data.
- 6 Governed & audited**
CloudTrail, Security Lake, GuardDuty, Audit Manager give the DoD ZT Pillar 4 trail across all accounts.

Zone Narrative

Edge Node

Amazon EKS Anywhere / Outposts run the full Kubernetes control plane locally, so Lux and the Neo-compiled model keep executing through a service-link drop. ECR ships one standardized image; KMS XKS / CloudHSM hold keys locally; S3 on Outposts is the on-node store.

Transport

AWS Ground Station provides managed downlink into GovCloud without owning antennas. Direct Connect / VPN and Transit Gateway interconnect the edge, landing, and security accounts — the node is a mesh participant, not a new central hop.

GovCloud Landing

Amazon S3 stores distilled results; Bedrock supplies in-Region model updates pushed to the edge opportunistically; EventBridge + Lambda fan out and process; RDS holds structured mission state.

Security & Compliance

CloudTrail + Security Lake provide the data-access audit; GuardDuty threat detection; Audit Manager + Config assemble NIST 800-53 / ZT evidence; KMS is the cryptographic root of trust for Pillar 4.

Severing the Tactical "Hairpin" Bottleneck

DoD Edge-Native Agentic AI Platform
Joint Capability: Scale AI • XQ Message • AWS

 THE OPERATIONAL PROBLEM

Routing telemetry to CONUS data centers creates fatal latency in contested space operations.

 SDA STRATEGIC SOLUTION

Autonomous agents fuse orbital sensor data and enforce zero trust at the sensor edge.

 Scale AI
The Tactical Brain

SDA Track Fusion: Correlates orbital sensor feeds in real time.
LUX Edge Runtime: Identifies orbital threats without cloud uplink.

 XQ Message
The Governance Engine

Cross-Echelon Sharing: Governs multi-classification space feeds.
Payload Security: Cryptographically binds Zero Trust to telemetry.

 AWS
The Secure Backbone

Sovereign Fabric: Forward-deployed tactical edge nodes.
IL-6 Clearance: Extends to GovCloud and Top Secret regions.

SDA
Demonstration:



Orbital Edge AI: Sensor-level tracking without cloud dependencies



Coalition Zero Trust: Cross-domain telemetry encrypted to payload



Outcomes

- **Elimination of Latency Penalties:**
 - **Mission Outcome:** Bypassing the round-trip "hairpin" route directly eliminates distance-induced latency, delivering real-time actionable data straight to the warfighter when seconds matter.
- **Operational Resilience in Contested (DDIL) Environments:**
 - **Mission Outcome:** Local data protection and validation mean tactical assets remain fully functional even when central connectivity is lost, transforming a potential liability into a reliable, edge-native capability.

Why This is the Right Solution:

This architecture represents the only viable path to achieving the DoD's operational and compliance requirements simultaneously.

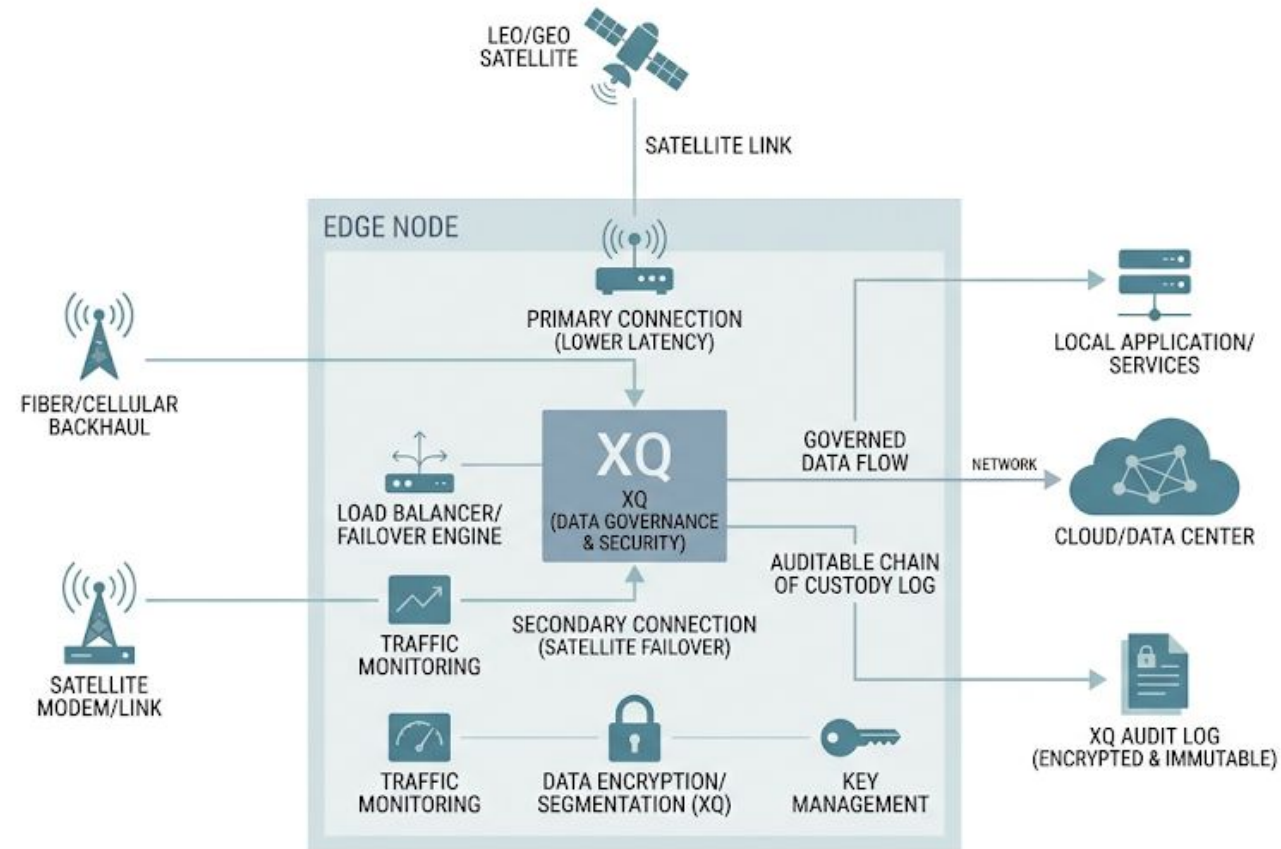
The joint capability Scale AI, XQ, AWS provides a direct instantiation of the DoD FY2027 Zero Trust mandate, specifically emphasizing Pillar 4 (Data). XQ + Scale LUX's AI capabilities purpose-built for the edge, meets the unique requirements of Space Domain Awareness by enabling secure AI-driven decisions across classified, disconnected, satellite, and commercial environments while enforcing data-level sovereignty and Zero Trust controls.

Appendix

BOX program intake: [BOX Feasibility Study submission form](#)

FailOver

Connectivity Failover with consisted access auditability.

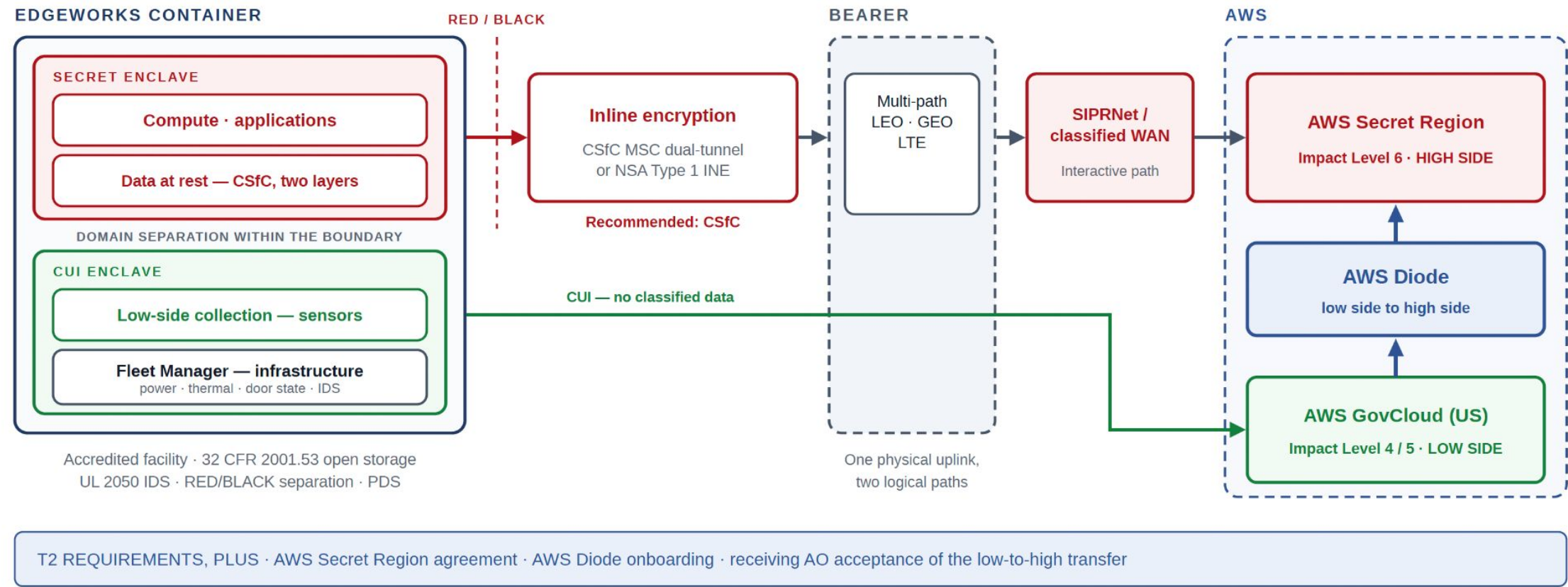


ATCO Edgeworks

TOPOLOGY 3

Secret Hybrid

Container holds Secret collateral and a low-side domain. Cross-domain transfer happens in AWS, not in the container.



Compliance & Zero Trust Mapping

DoD Zero Trust — Pillar 4 (Data)

XQ per-payload encryption + policy; AWS KMS, CloudTrail, Security Lake as the data-pillar controls.

Impact Level — IL5 / IL6

GovCloud (US) for IL5; AWS Secret Cloud (IL6) for classified workloads.

NIST 800-53 / 800-207

Audit Manager + Config map 800-53 controls; IAM Roles Anywhere provides 800-207 non-human identity.

ITAR + data sovereignty

GovCloud (US) ITAR-eligible; KMS External Key Store gives each nation jurisdictional key custody.

DDIL operational assurance

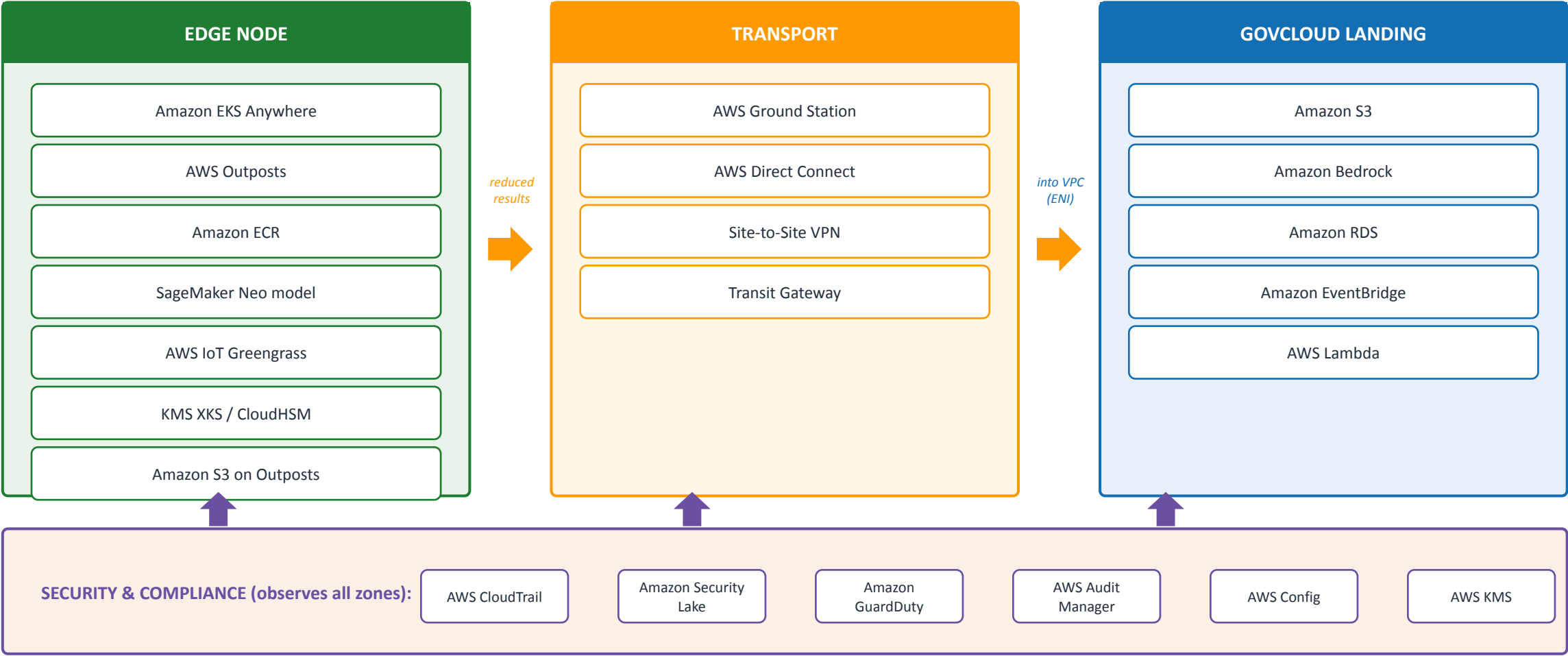
EKS Anywhere offline execution; Fault Injection Service scripts the link-denial acceptance test.

Key custody

XQ + KMS XKS / CloudHSM keep keys local; XKS suits custody (low-TPS), not bulk throughput.

AWS Service Architecture by Zone

● Edge ● Transport ● GovCloud landing ● Security & compliance *Data flows left → right; the Security & Compliance account observes all zones.*



Documentation References

Authoritative AWS documentation for each service in this architecture (click to open).

[Amazon EKS Anywhere](#)

[AWS Outposts](#)

[Amazon SageMaker Neo](#)

[AWS IoT Greengrass](#)

[Amazon Bedrock](#)

[AWS Ground Station](#)

[AWS KMS + External Key Store](#)

[AWS CloudHSM](#)

[AWS CloudTrail](#)

[Amazon Security Lake](#)

[Amazon GuardDuty](#)

[AWS Audit Manager](#)

[AWS Config](#)

[Amazon S3](#)

[Amazon EventBridge](#)

[AWS Fault Injection Service](#)

[AWS Nitro System security design](#)

[AWS GovCloud \(US\)](#)

BOX program intake: [BOX Feasibility Study submission form](#)