The Logic of Containment

12 axioms. One inevitable conclusion.

1

Trust will be violated in any system of sufficient complexity.

FIRST PRINCIPLE

2

Detection requires distinguishability. You cannot detect what looks normal.

LOGICAL PROPERTY

3

A centralized inspection point can only govern traffic that traverses it.

NETWORK PHYSICS

4

The internet is architecturally open. The default state is reachable.

PROTOCOL DESIGN

5

Cloud infrastructure is permissive by default.

VERIFIABLE FACT

6

The shared responsibility model places interior security on the tenant.

CONTRACTUAL FACT

7

The majority of cloud workloads are not segmented.

MEASURED REALITY

8

AI offensive capability is an emergent property of general AI improvement.

EMERGENT PROPERTY

9

Released information cannot be un-released.

INFORMATION PHYSICS

10

Containment is architecturally independent of detection.

ARCHITECTURAL PRINCIPLE

11

Ephemeral workloads cannot be secured by models that assume persistence.

TIMING CONSTRAINT

12

Attack surface exploitation scales with the number of capable attackers.

ECONOMIC REALITY

THEREFORE

The only architecturally sound response is containment that is independent of detection, that can secure workloads regardless of their lifespan, and that limits blast radius before any other system is involved.