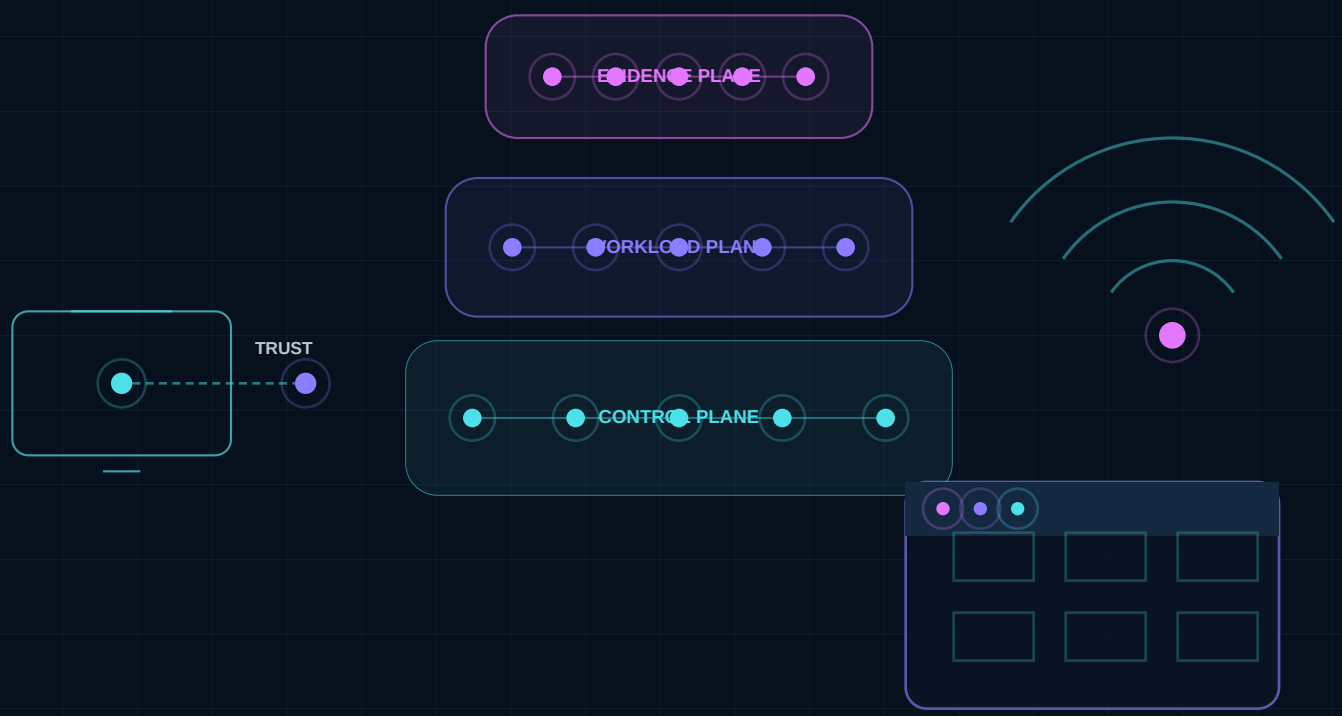
MYTHOS SYSTEMS

EXECUTIVE PORTFOLIO

Cloud, Edge, Hardware, Media, and Web Executive Portfolio

Leadership view of 21 permanent infrastructure standards spanning cloud control planes, managed endpoints, OT, telecommunications, trusted compute, IoT, realtime media, and browser isolation.



MYTHOS-CLOUDEDGE-EXEC-0001

PERMANENT PUBLICATION IDENTITY / CANDIDATE PUBLICATION / PUBLIC

Infrastructure assurance as one system

STANDARDS
21

ATOMIC CRITERIA
378

DOMAINS
8

GUIDES
3

FIELD GUIDES
8

RESEARCH
7

ARCHITECTURES
7

EVIDENCE MODEL
FOUNDATION

Eight domains, one control fabric

CLD	Cloud planes & workload placement
END	Endpoint trust & fleet state
OT	Zones, conduits & safety
TEL	RAN, RF, voice & timing
HW	Compute fabrics & firmware trust
IOT	Sensor identity & lifecycle
MED	Realtime media & provenance
WEB	Browser/runtime isolation

Policy gates every transition

Cloud, endpoint, OT, telecom, hardware, IoT, media, and browser systems are not separate risk islands. Identity, policy, state, telemetry, recovery, and evidence cross every boundary.

Failure propagation leaders must see

AUTHORITY DRIFT

Provider or device state diverges from approved policy.

HIDDEN DEPENDENCY

Cloud, firmware, carrier, browser, or supply-chain dependency fails outside local control.

UNVERIFIED RECOVERY

Failover exists on paper but restore, rollback, or degraded-mode behavior is untested.

TELEMETRY BLINDNESS

Observed health does not cover actual user, process, safety, or media outcome.

TRUST COLLAPSE

Identity, key, attestation, firmware, or update trust is compromised at scale.

Sequence the program around evidence

1

Inventory & classify

Assets, services, identities, zones, dependencies, versions, and owners.

2

Establish control planes

Policy, access, configuration, lifecycle, and source-of-truth boundaries.

3

Instrument reality

Telemetry across workload, device, process, RF, media, hardware, and browser state.

4

Prove failure behavior

Negative tests, overload, partition, rollback, restore, isolation, and safety cases.

5

Reconcile & govern

Compare intended, deployed, observed, historical, and exceptional states continuously.

Questions that gate material deployment

Q01

Can we name the authoritative control plane?

Q02

Can we prove identity and policy at the enforcement point?

Q03

Can we see degraded and unsafe states before users do?

Q04

Can we revoke, isolate, rollback, restore, and reconstruct?

Q05

Can we prove what happened from preserved evidence?

Q06

Can we exit the provider, platform, device, or protocol without losing control?

Candidate standards with bounded claims

This portfolio is a permanent Mythos library view. It does not replace the independently citable standards, guides, research reports, or reference architectures. Candidate status does not imply certification, regulator approval, or external validation.

PERMANENT IDENTITY

STABLE

Revisions retain the same public document identities unless scope changes create a genuinely new publication.

EVIDENCE POSTURE

REQUIRED

Claims are bounded by scope, version, environment, source currency, test period, and assessor confidence.

PRODUCTION METADATA

PRIVATE

Internal package or production sequencing never appears as public publication identity.

REVIEW TRIGGER

EVENT + CADENCE

Provider, protocol, firmware, browser, radio, or authority changes may trigger review before the scheduled date.