Elysium
NETWORK

• PUBLIC TECHNICAL WHITE PAPER

Enterprise Sovereign *Compute Plane*

Building private, governed AI infrastructure from existing enterprise devices.

AUTHORS

Mathis Young · Co-Founder & CTO · Alex Jenkins · Co-Founder & CEO

DOCUMENT

EYL-WP-2026-07 / v1.0

§ 01 — EXECUTIVE SUMMARY

Activate the compute you already own.

Enterprises, universities, and governments face rising demand for AI, security, governance, and cost control. The reflex is to purchase more infrastructure — GPUs, clusters, cloud commitments. Meanwhile, thousands of AI-capable PCs, workstations, GPU servers, and edge devices sit underutilized inside the same organization.

> *“Without a control plane, a fleet is only a fleet. It is not a compute platform.”*

SIX CORE PRINCIPLES

The operating model

01 **Customer ownership**
Devices, policies, and data placement remain under the organization’s control.

02 **Enterprise governance**
Identity, RBAC, policy, and audit built into the operating model.

03 **Heterogeneous infrastructure**
Windows PCs, Linux servers, GPU systems, AI PCs, and edge devices.

04 **Software-defined orchestration**
Capacity is delivered through software, not new construction.

05 **Security by design**
Identity, signed instructions, encryption, node health, admin approval.

06 **AI compatibility**
Inference, vision, rendering, simulation via APIs, SDKs, and gateways.

§ 02 — ENTERPRISE AI INFRASTRUCTURE

The problem is not compute shortage. *It is fragmentation.*

An enterprise may own thousands of devices, yet lack the software layer to organize them. Traditional infrastructure planning still assumes compute is delivered from a centralized environment — data center, colo, private cloud, or public cloud — creating six recurring constraints.

01 PROCUREMENT
Hardware selection, purchase, install, and support takes months.

02 CAPITAL COST
Accelerators, networking, power, cooling and support are expensive.

03 BURSTY DEMAND
High peaks with long troughs leave dedicated clusters underused.

04 CLOUD OPEX
Inference, egress, and managed services create unpredictable bills.

05 DATA RESIDENCY
Regulated sectors need control over where processing happens.

06 AI PC FLEETS
NPUs and CPUs on endpoints sit isolated, capturing a fraction of value.

QUESTIONS A FLEET CANNOT ANSWER WITHOUT A CONTROL PLANE

Which devices are available? · Which are approved to participate? · What are their capabilities? · Which are healthy & trusted? · Which workloads may run where? · How is work distributed & verified? · How is activity audited?

§ 03 — UNDERUTILIZED HARDWARE

Endpoints are managed as assets. Elysium treats them as *capacity.*

Unused capacity has no value unless it can be discovered, governed, scheduled, and measured. Elysium treats enterprise-owned devices as potential members of a governed compute plane. Participation is controlled — the institution decides which assets may join, which workloads they accept, when they may operate, and what security requirements apply.

A PC refresh becomes
a capacity-expansion cycle.

A GPU workstation becomes
an inference node when idle.

A computer lab becomes
a nighttime research resource.

A branch or plant becomes
a local compute fabric.

POLICY-DRIVEN MATCHING

Categories the platform considers

- ◇ Device class
- ◇ GPU availability
- ◇ Memory
- ◇ Network quality
- ◇ Administrative group
- ◇ Availability window
- ◇ Security posture
- ◇ Enterprise policy
- ◇ Processor capability
- ◇ NPU availability
- ◇ Storage
- ◇ Operating system
- ◇ Location
- ◇ Node health
- ◇ Workload eligibility

— *scoring proprietary*

Elysium does not merely connect devices. It organizes them into an operationally useful, governable compute resource.

§ 04 — THE PLATFORM

A software-defined enterprise compute platform.

Its purpose is to allow organizations to create private, customer-controlled compute capacity from infrastructure they already own or manage.

01 INTERFACE

Enterprise Console

Administration, visibility, and operational reporting for the entire compute plane.

02 ORCHESTRATION

eDOS Control Plane

Intake, policy, scheduling, monitoring, retries, aggregation, and audit.

03 EXECUTION

Node Agents

Installed on approved devices; enforce local limits and controlled runtimes.

04 ACCESS

Compute Gateway

REST APIs, SDKs, CLIs, webhooks, and AI-agent endpoints for applications.

05 TRUST

Security & Trust Layer

Identity, authorization, workload signing, encryption, and node validation.

06 RESULT

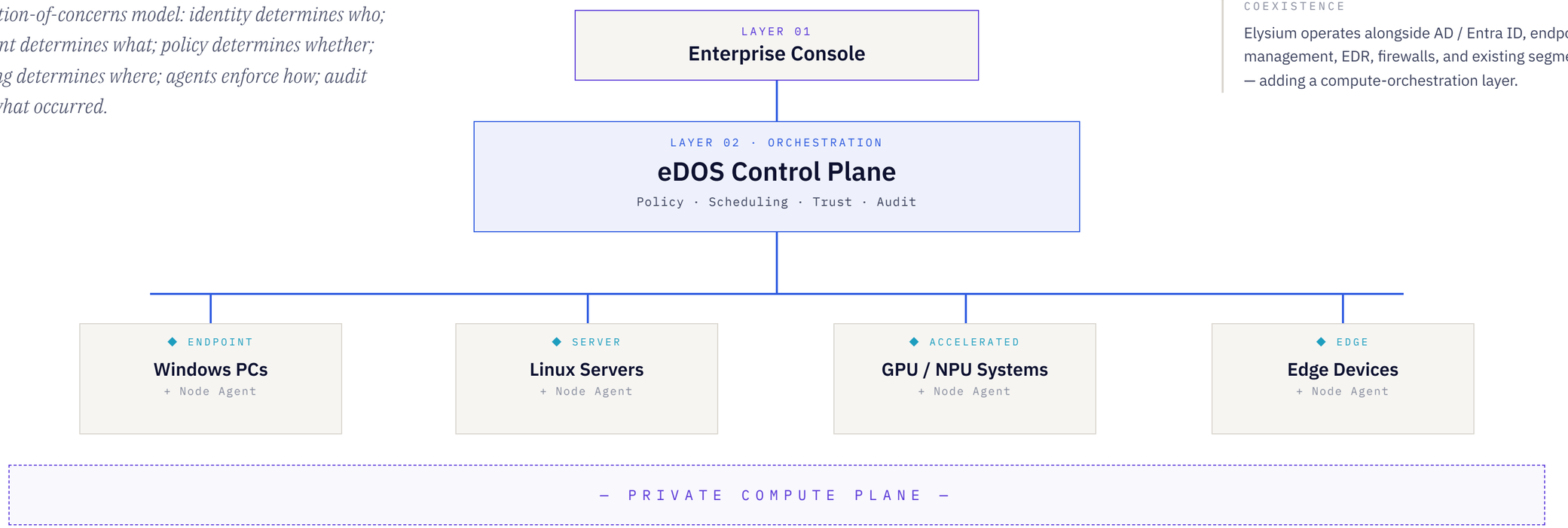
Private Compute Plane

The governed logical pool of approved enterprise-owned systems.

§ 05 — HIGH-LEVEL TOPOLOGY

Centralized governance. *Distributed execution.*

A separation-of-concerns model: identity determines who; enrollment determines what; policy determines whether; scheduling determines where; agents enforce how; audit records what occurred.



COEXISTENCE

Elysium operates alongside AD / Entra ID, endpoint management, EDR, firewalls, and existing segmentation — adding a compute-orchestration layer.

§ 06 — OPERATIONAL SURFACES

The face and the engine.

A THE FACE

Enterprise Console

Makes distributed infrastructure understandable through a centralized graphical environment.

FLEET

Fleet Overview
Enrolled nodes, capacity, utilization trends.

NODES

Node Management
Identity, class, OS, capabilities, heartbeat, health.

JOBS

Workload Management
Owner, type, priority, status, retries, output.

POLICY

Policy Management
Allowed classes, eligibility, data placement, quotas.

IAM

Identity & Access
Users, roles, IdP integration, access review.

AUDIT

Audit & Compliance
Admin actions, workload events, security events.

SERVES → INFRA · SECURITY · APP TEAMS · EXECUTIVES · RESEARCHERS · AUDITORS

B THE ENGINE

eDOS Control Plane

Coordinates intake, policy, node selection, execution, and results.

RESOURCE POOLS

General CPU	High-Memory	GPU Inference
AI PC	NPU-Capable	Research
Department	Site-Specific	Restricted-Data
Edge	Validation	+ custom

POOLS EXPRESS OPERATIONAL INTENT

A university permits research jobs only on research-pool devices. A healthcare organization restricts sensitive workloads to a private zone. A manufacturer keeps vision jobs local to the plant.

§ 07 — NODE AGENTS

A managed service. *Not remote control.*

The node agent executes workloads through controlled runtimes and defined permissions — never unrestricted remote access. Elysium is designed to use available capacity without disrupting the device's primary business role.

◇ RESPONSIBILITIES

- Register device with the environment
- Establish trusted relationship with control plane
- Report approved capability information
- Send periodic health & availability
- Receive only authorized workloads
- Enforce local resource limits
- Monitor thermal, memory, network, power
- Execute supported workload runtimes
- Return status and results
- Maintain audit-relevant execution records
- Suspend when policy or health requires it

◇ RUNTIME CLASSES

SANDBOXED
WebAssembly workloads

ISOLATED
Containerized workloads (where supported)

AI
Inference runtimes · ONNX-compatible models

BATCH
Approved scripts · data-processing jobs

MEDIA · SCI
Media transformation · scientific compute

Support ≠ eligibility. Every node × workload pair is gated by policy, capability, and admin approval.

▲ SAFETY CONTROLS

CPU cap	GPU cap
Memory cap	Battery floor
Thermal ceiling	Allowed hours
Network rules	Idle-required
User-session aware	Maintenance mode
Emergency stop	Allowlists

Enterprise endpoints have primary business purposes. Elysium uses available capacity without disrupting the device's normal role.

§ 08 — DISCOVERY, ENROLLMENT, IDENTITY

Discovery finds a device. *Enrollment authorizes it.*

ENROLLMENT PROCESS

01 Device identification
02 Administrative approval
03 Agent installation
04 Device registration
05 Identity validation
06 Policy assignment
07 Capability assessment
08 Trust establishment
09 Resource-pool placement
10 **Operational activation**

DISCOVERY SOURCES

Active Directory · Microsoft Entra ID · Endpoint management · Device inventories · CMDBs · Server inventories · Site processes · Manual enrollment

ROLE-BASED ACCESS

Enterprise roles at a glance

Platform Administrator
Global configuration · IdP integration · system control

Security Administrator
Access · audit · restrictions · security review

Researcher
Approved research on specific resource pools

Business Viewer
Utilization, capacity, and operational reports

Infrastructure Operator
Node groups · health · capacity · maintenance

Developer
Submit workloads through approved APIs and tools

Auditor
Review logs & reports · read-only

Finance devices reject research jobs · student labs run only approved educational work · engineering workstations participate outside business hours · GPU servers reserved for high-priority workloads.

§ 09 — CONCEPT

A logical, governed pool of customer-managed devices.

Sovereignty is not just where hardware sits. It is who owns the infrastructure, who administers the platform, who may access workloads, where data travels, and which external dependencies are required.

HOW IT DIFFERS FROM PUBLIC COMPUTE MARKETS

OWNERSHIP	Customer-owned or expressly authorized devices only
POLICY	Institution controls who, what, where, when, and how much
DATA BOUNDARIES	Customer defines where workloads and data may travel
IDENTITY	Enterprise users, groups, and roles — not anonymous participation
ADMINISTRATION	Control plane runs inside the customer's managed environment
NO TOKEN ECONOMY	No public cryptocurrency or open-market bidding required
AUDITABILITY	Every administrative and workload event is reviewable

LOGICAL SUB-PLANES

One plane. Many contexts.

Corporate General
Approved internal workloads across office systems

Research
University or laboratory contexts

Restricted
Regulated or sensitive workloads

Edge
Branch · plant · campus · field locations

GPU
Accelerated inference, rendering, scientific

AI PC
NPU-, GPU-, CPU-enabled endpoints

§ 10 — ORCHESTRATION & EXECUTION

From request to result, *in ten phases.*

PHASE 01

Submission

Console, API, SDK, CLI, webhook, or AI agent submits a request.

PHASE 02

AuthN & AuthZ

Confirms identity and whether it may request this workload.

PHASE 03

Policy Validation

Type, runtime, resource, location, and quota rules evaluated.

PHASE 04

Resource Matching

Eligible nodes identified by capability, health, trust, and zone.

PHASE 05

Task Distribution

Workload packaged into tasks, distributed to selected nodes.

PHASE 06

Execution

Agents run tasks within assigned resource & security limits.

PHASE 07

Monitoring

Progress, timeouts, health, and policy state tracked live.

PHASE 08

Retry / Recovery

Failures reassigned or stopped per policy.

PHASE 09

Result Handling

Returned, validated, aggregated, delivered to destination.

PHASE 10

Audit & Reporting

Operational, security, and governance events recorded.

§ 11 — COMPUTE GATEWAY

Accessible to applications. *Not just to administrators.*

An application should not need to know the network address of every participating workstation. It submits a request, specifies requirements, and lets the control plane decide where the work belongs.

INTEGRATION PATTERNS

Synchronous request

Application submits a short-running task and waits for the result.

Asynchronous job

Submits a longer workload, receives a job ID, polls status later.

Event-driven workload

A webhook or event triggers a workload automatically.

Batch submission

Large set of tasks submitted for distributed processing.

AI agent tool

An AI agent requests a permitted operation through a controlled function.

Pipeline integration

A workflow platform sends one stage of a data or AI pipeline.

Hybrid routing

Workload is evaluated for execution on customer-owned infrastructure, dedicated servers, or an approved external provider.

INTERFACE SURFACES

- REST APIs
- SDKs
- Command-line tools
- Webhooks
- Application connectors
- Internal service integrations
- AI agent integrations
- Workflow automation
- Developer portal

§ 12 — LAYERED CONTROLS

Security is not an add-on.

It is the condition that makes distributed compute possible.

L1 · IDENTITY
Identity
Users, admins, services, devices — all require an identity.

L1 · AUTHZ
Authorization
Role, pool, workload, device group, and policy scoped.

L2 · TRUST
Device Trust
Enrolled and recognized — identity, capability, health.

L2 · WORKLOAD
Workload AuthZ
Nodes accept only workloads authorized by the control plane.

L3 · INTEGRITY
Signed Instructions
Authenticated, integrity-protected workload dispatches.

L3 · CRYPTO
Encryption
Communications in transit; sensitive data at rest.

L4 · POLICY
Policy Enforcement
Rules define who, what, where, when, and how much.

L4 · AUDIT
Audit Logging
Admin actions, workload events, enrollment, access.

L5 · ISOLATION
Resource Isolation
OS-appropriate mechanisms for each runtime.

L5 · HEALTH
Node Health
Unhealthy or non-compliant nodes removed from scheduling.

L5 · LOCALITY
Data Placement
Restrict workloads to approved pools, locations, zones.

L6 · CONTROL
Revocation
Disable users, nodes, keys, policies, or workload access.

ZERO-KNOWLEDGE POSITIONING

Elysium is designed so it does not require access to unrelated user content in order to schedule and manage compute. Not a claim of cryptographic zero-knowledge proofs.

COMPLIANCE SUPPORT

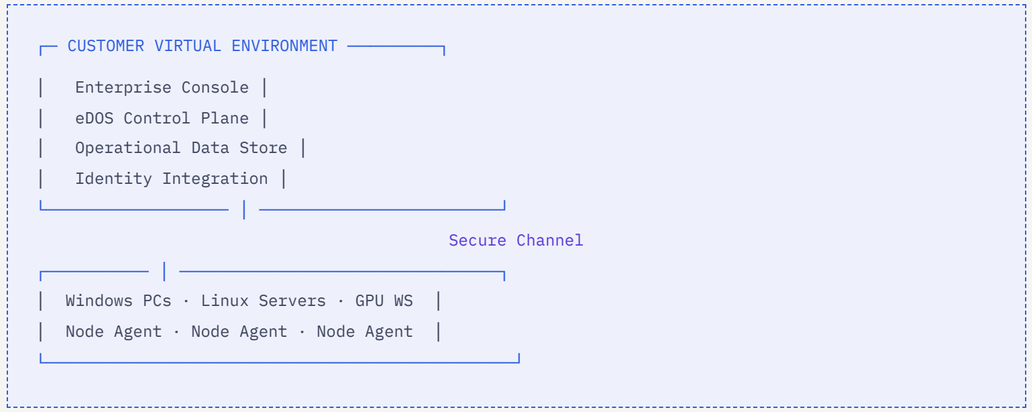
Technical capabilities that support institutional programs — FERPA-conscious, HIPAA-conscious, sector-specific. Compliance remains a shared responsibility.

§ 13 — ENTERPRISE DEPLOYMENT

Fit into what exists. *Don't replace it.*

PILOT TOPOLOGY

Start controlled. Prove operations.



- ◇ 10–25 devices
- ◇ One approved workload
- ◇ One operating window
- ◇ One admin team
- ◇ One resource pool
- ◇ Defined success criteria

DEPLOYMENT PATTERNS

Single-Site Private	Control plane and nodes operate within one site.
Multi-Site Enterprise	One control plane spans offices, campuses, regions.
Departmental	A business unit or lab runs its own compute plane.
Sovereign	Deployed entirely inside customer-controlled infrastructure.
Hybrid	Owned capacity combined with dedicated or external compute.
Edge	Local nodes and control services for low-latency remote sites.

A production deployment adds HA control-plane services, multiple pools, monitoring, backup, change management, and lifecycle governance.

§ 14 — WORKLOAD CATEGORIES

What runs on the plane.

ACCELERATED

AI Inference

Classification · Embeddings · Summarization · Vision · Anomaly detection · Recommendation · Local model exec · Agent tools

VISION

Computer Vision

Object detection · Image classification · Quality inspection · Frame processing · Document image analysis

DOCS

Document Processing

OCR · Text extraction · Format conversion · Classification · Indexing · Metadata generation

RESEARCH

Scientific Computing

Simulation · Statistical processing · Parameter sweeps · Numerical analysis · Data transformation

MEDIA

Rendering & Media

Video transcoding · Image rendering · 3D rendering · Audio processing · Media conversion

ANALYTICS

Analytics

Batch analytics · Data cleaning · Feature generation · Log processing · ETL steps

AUTOMATION

Software & Automation

Build tasks · Test execution · Validation · Data transformation · Scheduled automation

EDUCATION

Educational & Research

Universities providing controlled access to compute for approved learning and research activities.

*Elysium is designed to **complement**, not replace, every form of HPC. Workloads requiring tightly coupled interconnects, ultra-low latency, or massive shared memory belong in dedicated clusters.*

§ 15 — WHERE IT LANDS

Nine industries.
One operating model.

01 Higher Education

Campus-owned compute plane · student access · research support · AI experimentation · reduced immediate cluster expansion.

02 Government

Sovereign infrastructure · agency-controlled compute · site-specific placement · reduced external dependency · edge + field.

03 Healthcare

Customer-controlled infrastructure · local execution · policy-based data placement · better use of existing workstations.

04 Manufacturing

Local computer-vision · engineering simulation · predictive maintenance · plant-level compute · lower-latency analysis.

05 Financial Services

Private AI inference · batch analytics · model validation · risk processing · controlled distributed execution.

06 Defense & Aerospace

Sovereign deployment · restricted resource pools · edge inference · simulation · secure administration.

07 Media & Entertainment

Distributed CPU/GPU capacity for rendering, encoding, transformation, and content processing pipelines.

08 Retail

Branch, store, warehouse, and corporate systems for approved analytics, vision, forecasting, and automation.

09 Telecommunications

A software orchestration layer across enterprise, edge, and site infrastructure at operator scale.

Each industry requires its own security, performance, governance, and operational design — the platform is the common substrate.

§ 16 — VALUE MODEL

The case begins with *utilization.*

$ ECONOMICS

Return on assets already owned

- Delay some infrastructure purchases
- Reduce demand for always-on cloud capacity
- Use existing systems for burst workloads
- Extend device value beyond primary role
- Consolidate duplicate departmental infrastructure
- Create a visible, shared enterprise compute layer

> *Elysium does not claim cloud or data-center spend can be eliminated. It offers another option: use eligible existing capacity before purchasing more.*

SUSTAINABILITY

Use what already exists

Higher hardware utilization	Delayed equipment replacement
Lower embodied-carbon impact	Reduced electronic waste
More efficient facility use	Reduced data movement

EVIDENCE-BASED REPORTING

Utilization before/after · work on existing HW · cloud avoided · purchases delayed · energy per workload · participation hours · carbon by location · lifecycle extension

§ 17 — MARKET POSITION

Not another cloud.
A new compute layer.

ALTERNATIVE MODEL	WHAT IT DOES	WHERE ELYSIUM SITS
Public Cloud	Broad, elastic infrastructure operated by the provider.	Customer-owned or customer-managed compute. Coexists.
Traditional Data Centers	Centralize servers, storage, power, cooling, operations.	Distributed enterprise devices as an additional compute tier.
Dedicated GPU Clouds	External access to accelerated infrastructure.	Orchestrates devices under the customer's control.
Public Compute Marketplaces	Aggregate third-party hardware from independent providers.	Enterprise enrollment · private admin · policy · governed nodes.
Traditional Virtualization	Consolidate workloads on server infrastructure.	Extends orchestration to endpoints, AI PCs, edge devices.
Endpoint Management	Deploy software, enforce configuration, secure devices.	Uses managed endpoints as potential compute nodes.
HPC Clusters	Tightly integrated, high-performance environments.	Best for workloads distributable across heterogeneous nodes.

◆ Customer-owned HW ◆ Enterprise identity ◆ Private control plane ◆ AI-compatible gateway ◆ Sovereign options ◆ No public token

§ 18 — FUTURE DIRECTION

Ten trajectories under continued development.

01 **AI PC Orchestration**
Expanded support for enterprise AI PCs as managed compute nodes.

02 **NPU Support**
Broader ability to identify and schedule workloads to neural-processing units.

03 **Enterprise Discovery**
Deeper integration with directories, endpoint management, and CMDBs.

04 **Runtime Expansion**
More approved runtimes: AI, containers, WebAssembly, scientific, automation.

05 **Hybrid Capacity**
Owned infrastructure first, approved overflow to dedicated or external.

06 **Advanced Policy**
Finer rules for location, data class, resource use, identity, priority.

07 **Trust & Attestation**
Expanded device validation and hardware-backed trust signals.

08 **Observability**
Capacity analytics, energy visibility, and operational monitoring.

09 **Developer Ecosystem**
SDKs, APIs, connectors, CLIs, and integration patterns for AI agents.

10 **Enterprise Operating Experience**
Continued eDOS development as the managed operating environment.

Features described may be under development, available in pilot, or planned for future releases. This paper does not create a warranty or roadmap commitment.

§ 19 — CONCLUSION

The next phase will not be built only in hyperscale data centers.

It will also be built from the devices organizations already own.

Elysium is not presented as a replacement for every cloud, data center, cluster, or specialized platform. It is a new enterprise compute layer — designed to activate capacity that already exists and make that capacity useful, governable, and accessible.

Elysium
NETWORK

CONTACT

Mathis Young
Co-Founder & Chief Technology Officer

Alex Jenkins
Co-Founder & Chief Executive Officer

www.elysiumnetwork.io