

EdgeNebula Security Architecture

1. Executive Summary

EdgeNebula provides a private, distributed compute fabric designed for **artificial intelligence (AI) inference** and **latency-sensitive workloads**.

Unlike shared public cloud environments, EdgeNebula provides **deterministic, dedicated compute, explicit geographic placement control** and **transparent operational governance**. This enhances sovereignty, clarifies audit boundaries and reduces cross-tenant exposure risks.

Security is embedded across physical, network, compute, and operational layers. This includes dedicated compute environments, private network mesh architecture, hardware-level supply chain assurance, encrypted communications, and continuous telemetry monitoring.

The architecture prioritises isolation, sovereignty, resilience, and auditability for regulated and enterprise workloads and is designed to support compliance with recognised frameworks including ISO 27001 control families, SOC 2 principles, UK GDPR requirements, and industry best practices in cyber and physical security.

2. Security Design Principles

EdgeNebula's security architecture is guided by the following principles:

- **Isolation by Design** – Dedicated or logically segregated compute environments with controlled scheduling and no uncontrolled cross-tenant execution.
- **Least Privilege Access** – Role-based access controls (RBAC) enforced across infrastructure and management layers.
- **Defence in Depth** – Layered controls across physical, network, system, and operational domains.
- **Sovereign Control** – Infrastructure deployed in jurisdictionally controlled environments with defined data residency.
- **Operational Transparency** – Continuous telemetry, logging, and auditable monitoring.
- **Secure Supply Chain** – Vendor verification, firmware validation, and hardware provenance controls.

3. Threat Model

The EdgeNebula security architecture considers adversaries including:

- Opportunistic internet-based attackers
- Privileged insider threats
- Supply chain compromise actors
- Advanced persistent threats operating within defined jurisdictional constraints

Security controls are designed to mitigate unauthorised access, lateral movement, privilege escalation, data exfiltration, denial-of-service conditions, and firmware-level compromise.

4. Physical Security

EdgeNebula deployments incorporate:

- Controlled facility access (multi-factor authentication where applicable)
- CCTV and environmental monitoring
- Tamper-evident hardware and enclosure controls
- Segregated access zones for customer equipment

Physical access to customer hardware is restricted and auditable.

5. Network Architecture & Isolation

EdgeNebula utilises a private network mesh architecture to interconnect modular nodes while maintaining strict segmentation.

Key controls include:

- Segmented tenant network overlays
- Private interconnects independent of public internet routing
- Firewall enforcement at ingress and egress boundaries
- Software-defined networking (SDN) controls
- Encrypted communications between nodes

No uncontrolled cross-tenant traffic routing is permitted.

6. Compute & Virtualisation Controls

EdgeNebula deployments are structured to prevent uncontrolled resource contention and cross-tenant exposure.

Controls include:

- Dedicated resource allocation in single-tenant deployments
- Contractually defined oversubscription policies where applicable
- Hardened hypervisor configurations
- Secure boot enforcement
- Firmware integrity validation

GPU partitioning features (e.g., MIG) are deployed in accordance with workload isolation requirements.

7. Cooling & Infrastructure Stability

EdgeNebula supports direct-to-chip and immersion liquid cooling architectures. These systems provide enhanced thermal stability under sustained high-density AI workloads, reducing operational stress and improving reliability.

Cooling architecture is integrated into infrastructure monitoring systems to maintain predictable operating conditions.

The infrastructure is supported by Uninterruptible Power Supply (UPS).

8. Identity & Access Management

Access to management systems is governed by:

- Role-based access control (RBAC)
- Multi-factor authentication (MFA)
- Segregation of administrative domains
- Centralised logging of access events

Integration with enterprise identity providers (e.g., Azure AD, Okta) is supported where required.

9. Encryption & Data Protection

EdgeNebula supports:

- Encryption in transit (TLS 1.2+ or equivalent)
- Encryption at rest where deployed by customer workload configuration
- Secure key management integration
- Customer-managed key options where applicable

Data ownership and encryption responsibility are defined within the shared responsibility model.

10. Monitoring, Logging & Incident Response

The platform supports continuous monitoring across:

- Power and environmental telemetry
- Network activity
- System logs
- Access events

Security events may be integrated with customer SIEM systems.

Incident response procedures are documented and aligned with industry-standard response practices.

Log retention and monitoring duration are configurable in accordance with customer and regulatory requirements.

11. Supply Chain Security

EdgeNebula enforces supply chain controls including:

- Approved vendor sourcing
- Firmware validation
- Hardware authenticity checks
- Secure boot verification
- Component traceability

Third-party suppliers are evaluated against defined security criteria.

12. Compliance & Governance

EdgeNebula aligns with recognised control frameworks including:

- ISO 27001 control domains
- SOC 2 Trust Services Criteria
- UK GDPR requirements
- Cyber Essentials Plus principles

Certification roadmap and audit documentation are available upon request.

13. Shared Responsibility Model

Security responsibilities are divided clearly:

Domain	EdgeNebula Responsibility	Customer Responsibility
Physical facility	✓	
Network segmentation	✓	
Hardware integrity	✓	
Workload security		✓
Application patching		✓
Identity governance	Shared	Shared

This model ensures clarity in operational and compliance ownership.

14. Conclusion

EdgeNebula’s security architecture integrates physical, network, compute, and operational controls into a unified framework designed for sovereign, high-density AI infrastructure.

The platform emphasises isolation, resilience, auditability, and regulatory alignment while enabling modular deployment across distributed environments.

Security is embedded in design, deployment, and operations — not added post-construction.