Superclusters Security Overview

Single-tenant by design /

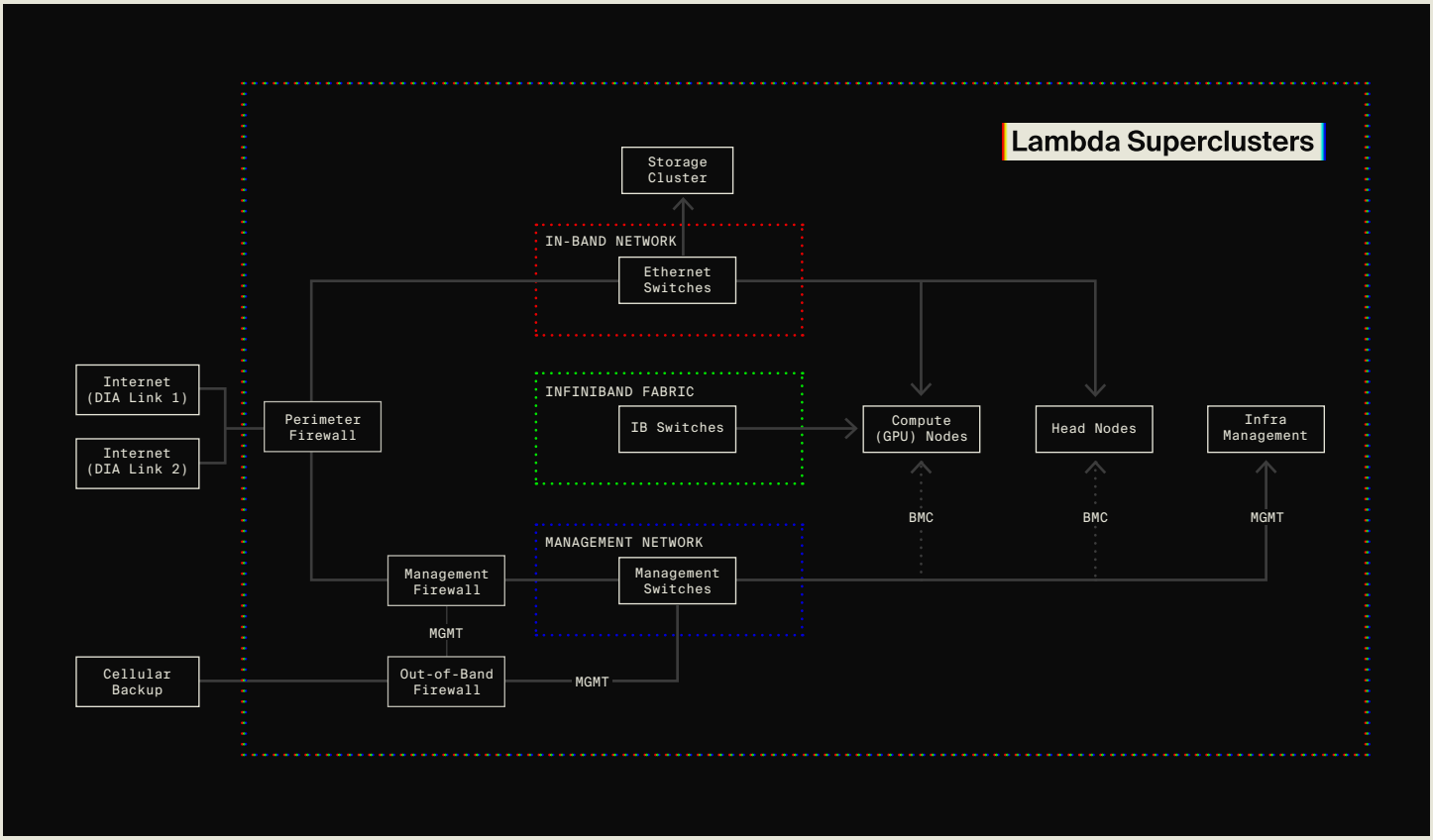
Lambda Superclusters are dedicated Single-tenant clusters with no shared components from the perimeter firewall down. Physical and logical isolation eliminates contention and inter-tenant risk.

Customer-controlled access /

+ **Customer Controlled:** Administrative control from day one
+ **Lambda access is revocable at any time:** once revoked, all cluster access is governed by customer controls.

Assurance /

+ **Completed:**
  + SOC 2 Type II (Security & Availability criteria)



Offering models & responsibility /

We offer a baseline dedicated cluster with optional managed services.
The matrix below clarifies who owns which controls.

Layer / Control Area	Bare-metal / Physical-only Support (Self-managed)	Managed Superclusters (Co-managed)	Managed Kubernetes (Fully-managed)
Tenant isolation	Dedicated compute, network and storage hardware; no shared cluster component	Same	Same
Physical security	Dedicated cabinets. DC guard staff, CCTV, multi-factor checkpoints, optional secure cage or dedicated data hall	Same	Same
Network perimeter	Customer-managed firewall (default deny inbound) with VPN/ peering options	Co-managed change workflows; Lambda proposes, customer approves	Integrated with k8s network policies
Management access	No standing Lambda logical access; you may grant time-boxed access as needed	Lambda retains tightly scoped access for operations, Lambda's access is **revocable by the customer at any time**	Lambda retains exclusive node management access, customer k8s access through SSO via OIDC/SAML with role-based access controls
OS & host hardening	Customer owns OS patching, users, keys, and logging	Joint: Lambda assists within coordinated maintenance windows; audit logs available	Lambda manages cluster and k8s control plane patching
Storage & keying	Networked storage encrypted at rest (AES-XTS 256-bit); customer controls access to data	Same; Lambda supports ops tasks with customer approval	Same
Monitoring & logging	Customer-provided tooling	Co-managed runbooks; logs and audit trails for Lambda actions	Integrated cluster logging and metrics
Support model	Break/fix hardware support via ticket system; no autonomous actions by Lambda.	Proactive operations per runbook with coordinated maintenance windows	Kubernetes and cluster lifecycle managed by Lambda

Technical specifications /

Physical security

[FACILITY & ENCLOSURE]

+ Dedicated cabinets with dedicated power, cooling, and network infrastructure.
+ Optional slab-to-slab hard-walled room or dedicated secure cage (tight mesh, roof, optional below-floor extension).
+ Customer-controlled badging and optional in-cage cameras.
+ Optional customer-assigned security personnel to guard access to the isolated area.

[CONTROLS & MONITORING]

+ 24×7×365 on-site security presence and surveillance; perimeter fencing and gated access.
+ Multi-stage checkpoints with mantraps and multi-factor access (badge + biometrics).
+ Self-closing, tamper-resistant doors/gates; ingress/egress and aisle cameras with ≥90-day retention.
+ Physical access logging with ≥1-year retention; access reviewed for maintenance and incidents.

Data security

+ **Encryption at rest:** Persistent storage utilizes **AES-XTS 256-bit** encryption. A unique key is generated at build time for your cluster; data on a physically removed drive is irrecoverable without that key.
+ **In-transit:** Storage traffic remains on your cluster's local network in normal operation (not encrypted by default). Application-layer encryption can be layered where required.
+ **Media control:** NIST 800-88 compliant data sanitization process at contract end, including physical destruction of obsolete or faulty storage media.

Logical security & platform hardening

[FIRMWARE & HOST BASELINE]

+ All nodes (compute, head, management) shipped with the latest validated BIOS and BMC firmware with secure BMC passwords.
+ All nodes provisioned with a current Ubuntu LTS release. The customer receives root access on all nodes via the initial SSH authorized key.

[NETWORK ARCHITECTURE]

+ In-band Ethernet network (all compute/management nodes + persistent storage) with redundant DIA links; perimeter firewall initially configured with no Internet-exposed ingress.
+ InfiniBand fabric (spine-leaf) for RDMA-optimized GPU communication; secure IB keys configured to prevent nodes from altering IB fabric configuration.
+ Management network for control plane systems, smart PDUs, device management interfaces, and BMC/DPUs; connectivity to in-band via a dedicated management firewall.
+ Out-of-band (OOB) network with its own firewall and a backup low-bandwidth Internet link for emergency device access; no general routing is allowed over the OOB.

[ACCESS OPTIONS - CUSTOMER-CONTROLLED]

+ **Client VPN** on the perimeter firewall for secure remote access.
+ **Site-to-site IPsec VPN** to your environment; optional IP allowlists on the outer tunnel.
+ **Private connectivity:** AWS Direct Connect, Azure ExpressRoute, GCP Interconnect, OCI FastConnect terminated at your perimeter firewall.
+ **Direct jump node** access (if preferred) via the Internet under your policies.

Technical specifications cont./

Compliance and assurance

+ **SOC 2 Type II (Security & Availability):** An independent assessment confirms that controls were suitably designed and operated effectively over the coverage period.
+ **Third-party risk management:** Lambda performs due diligence and continuous monitoring for all data centers in which we operate, reviewing providers' SOC 2 reports for alignment with Lambda's requirements.
+ **Trust Portal:** Centralized access (under NDA as applicable) to attestations/certifications, privacy & security practices, product security measures (e.g., penetration testing executive summaries), and other security documentation.

Customer controls & complementary responsibilities

To align with industry frameworks (e.g., SOC 2 CUECs/CSOCs), the following areas typically remain your responsibility unless otherwise scoped in a managed engagement:

+ Identity & access management (SSO/IdP, user lifecycle, MFA policies) for your users.
+ OS-level hardening, patching cadence, and endpoint controls on compute/head nodes (co-managed in the managed model).
+ Network security policies (firewall rules, VPN credential hygiene, peering/IPsec secrets management).
+ Logging/monitoring/SIEM integration and alerting for your workloads.
+ Data classification, application-layer encryption, and key management policies.
+ Approval for change control of maintenance windows and configuration updates.

Frequently asked assurances

+ **Can Lambda see our data?** Lambda has no logical access to your cluster or its data unless you grant us access or opt to utilize our Managed Kubernetes service.
+ **What happens at contract end?** All storage drives are sanitized in accordance with NIST 800-88 guidelines.
+ **How quickly can we cut off access?** Immediately: revocation of Lambda access is supported and entirely under your control.