

Technical Specifications

Infrastructure & Facilities

Where is MelroseINC Private Media Cloud (PMC) physically located?

MelroseINC Private Media Cloud is hosted at Equinix LA3 — part of the Equinix Los Angeles IBX cluster. Equinix is the world's largest data center operator. LA3 is a purpose-built facility for the media and entertainment ecosystem, serving 360+ companies with access to 75+ network providers and the second-largest peering exchange in Los Angeles.

What is the physical footprint of PMC at Equinix LA3?

Operational since 2021, MelroseINC currently operates two dedicated 8-cabinet cages within LA3. Both cages are fully owned and operated by MelroseINC. Expansion plans to additional Equinix locations are under development.

What are the facility specifications at LA3?

Equinix LA3 provides enterprise-grade infrastructure including:

- Power: Dual utility feeders, N+1 UPS configuration, 11 x 2,000 kW diesel standby generators (N+1 redundancy)
- Cooling: Air-cooled and water-cooled chillers with CRAC units, N+1 redundancy
- Physical Security: Mantrap entry, 24/7 on-site security officers, biometric readers, fiber vault, CCTV with 90-day retention, motion detection
- Fire Suppression: Double-interlocked pre-action dry pipe system with HSSD/VESDA detection
- Network: 10Gb network ports standard, high-availability firewall protection
- Reliability: >99.999% uptime track record globally

Who owns and operates the network and equipment within PMC?

All networking, switching, storage, and security equipment within PMC is owned and operated by MelroseINC. External internet connectivity is provided by three independent ISPs — Zayo, CrownCastle, and Cogent — ensuring redundant upstream paths. Equinix owns and operates the facility (power, cooling, physical security) as our colocation partner.

Security

What compliance certifications apply to PMC?

Our Private Media Cloud operates inside Equinix LA3, which is independently audited every year against:

- SOC 1 Type 2 and SOC 2 Type 2 (security and availability)
- ISO/IEC 27001:2022 (information security management)
- ISO 22301:2019 (business continuity management)
- ISO 9001:2015 (quality management)

Those facility certifications are held by Equinix as the data center provider. MelroseINC layers its own physical, network, and operational controls on top of that certified foundation. Equinix attestation reports are available on request for studio or vendor audits, and our own Information Security Policy — which names the independent auditor (Schellman), the SOC report periods, and the ISO certificate number and expiry — is available under NDA. Multiple MelroseINC PMC clients have successfully completed studio and TPN security audits with the assistance of our engineering team.

Technical Specifications (cont'd)

Who is responsible for security — Equinix, MelroseINC, or the client?

Responsibilities are divided across three layers, and the division is documented:

- Equinix (facility) — physical perimeter, power and redundancy, cooling, fire detection and suppression, and environmental monitoring.
- MelroseINC (managed infrastructure) — firewalls, network segmentation, tenant isolation, encrypted VPN, and the compute, storage, and connectivity underneath the environment, plus patching, hardening, monitoring, and incident response for everything we manage.
- Client (applications, data, users) — application configuration, user access, and data classification and retention. For colocation (client-hosted equipment), MelroseINC provides secured space, power, connectivity, and hands-on hardware support and does not hold administrative or logical access to client equipment. For managed and hybrid engagements, MelroseINC operates the managed infrastructure on the client's behalf while the client's own IT retains the application, data, and user layer; the precise split is defined in the service order.

What access controls protect the environment?

Access to our Private Media Cloud management systems follows least privilege. Accounts are individually assigned and role-based (RBAC), multi-factor authentication is enforced for remote and administrative access, access rights are reviewed periodically, and access is revoked promptly on role change or separation. Client environments are reachable only by that client's authorized users.

How is your staff vetted and trained?

Personnel with access to secured facilities undergo background screening consistent with applicable law, are bound by confidentiality obligations, receive security-awareness training on hire and periodically thereafter, and are subject to a formal onboarding and offboarding process that provisions and de-provisions access on a timely basis.

What is your firewall configuration standard?

Our PMC managed SonicWall Next-Generation Firewall (NGFW) is configured in accordance with the MPA Content Security Best Practices (v5.3.1) and the ISO 27001 framework, with intrusion detection and prevention (IDS/IPS) and the full security suite enabled by default. Firewall rules are audited regularly. Logging is handled via a Syslog server, with continuous network monitoring and 24/7 security operations center (SOC) monitoring and threat detection. MelroseINC conducts regular vulnerability assessments and penetration testing of the PMC environment.

How is each client's environment isolated from other tenants?

Client environments are isolated at the network level using dedicated VLANs and VRF (Virtual Routing and Forwarding) segmentation, with east-west traffic isolation between tenants. Storage access is isolated by VLAN, so only devices on a client's designated VLAN can reach that client's storage. While some logical management networks exist within the core PMC infrastructure, all client-facing traffic is isolated using these mechanisms.

How is data encrypted?

Data on MelroseINC-provided storage (On-Demand and managed Qumulo storage) is encrypted at rest by default. For client-owned colocated equipment, encryption at rest remains the client's responsibility, and our engineers are available to advise on the right approach. Remote access to our PMC is encrypted end to end with AES-256 over VPN; for clients who require it, we also offer a Zero Trust access model that verifies every user and device before granting access and enforces least privilege. Tenant environments are separated by VLAN and VRF isolation at the transport layer.

How are changes to production infrastructure managed?

Changes to MelroseINC-managed production infrastructure are reviewed, tested where practical, and documented under a formal change-management process. Clients receive one-week advance notice of scheduled maintenance affecting shared infrastructure.

Technical Specifications (cont'd)

How are security incidents handled?

MelroseINC maintains a documented incident-response process for detecting, containing, investigating, and remediating security events. We commit to notifying affected clients of any confirmed or reasonably suspected security incident affecting their data or equipment within 72 hours, and to cooperating fully with the client's own investigation and regulatory reporting. MelroseINC also carries cyber liability and technology errors & omissions insurance with limits of \$2 million per occurrence. Our incident-response process follows MPA and TPN framework guidelines.

How is media sanitized when equipment is decommissioned?

Media decommissioning for MelroseINC-owned assets follows secure sanitization and disposal practices, so data does not persist on retired drives or systems.

How do you manage third-party providers such as Equinix?

MelroseINC relies on Equinix as a named subservice organization for the data center facility and evaluates Equinix's controls through its independent SOC and ISO attestations. Other third-party providers are subject to due diligence review appropriate to the service they provide and the data they may access.

Do you provide network diagrams?

Network diagrams are available on request for clients hosting equipment at our PMC, and are provided post-contract as part of the onboarding process. Pre-deployment diagrams are provided on a case-by-case basis for qualified enterprise opportunities.

Networking & Connectivity

What switching and firewall hardware does PMC use?

MelroseINC's PMC network infrastructure is built on enterprise-grade, fully supported hardware:

- Core Switching: Arista Networks 7050TX3 and 7060CX3 Ethernet Switches — shared infrastructure with per-client VLAN/VRF isolation
- Managed Firewall: Next-Generation Firewall (NGFW)
- ISP Connectivity: Zayo, Crown Castle, and Cogent (multiple redundant providers)

All hardware is current, fully supported by active vendor agreements, and not end-of-sale or end-of-life. MelroseINC's lifecycle policy is to replace hardware when it reaches end-of-support status.

What bandwidth options are available?

Standard hosting configurations include 1GB bandwidth. Higher bandwidth allocations are available based on client requirements and are priced accordingly. There are no data egress fees, no overage charges, and no bandwidth throttling — PMC operates on a flat, transparent pricing model. Unlike public cloud providers, bandwidth costs are predictable and included in your monthly rate.

Can I access PMC remotely?

Yes. All MelroseINC PMC clients access their environments remotely via VPN. We support clients across the continental United States and internationally. Our infrastructure is designed for remote-first workflows — many of our clients have eliminated their physical office entirely and operate 100% through PMC.

Technical Specifications (cont'd)

Storage & Data Protection

What storage platform does PMC use?

Our PMC platform uses Qumulo, an enterprise-grade NAS (Network Attached Storage) platform with a clustered filesystem architecture. Qumulo provides high-performance, scalable storage specifically optimized for large media files and collaborative workflows. The platform is current, fully supported, and under active vendor maintenance.

How is storage redundancy handled?

Qumulo uses erasure coding within a clustered filesystem. The configuration is tolerant of 2x drive failures per node, or 1x full node failure per cluster — providing significant protection against hardware failure without data loss.

Is there default data protection?

Yes. Encryption at rest is enabled for all tenants using Qumulo storage, and storage is protected through Qumulo's erasure-coding redundancy (described above). Backup, disaster recovery, and immutable, ransomware-resilient recovery are available as managed add-ons, scoped per client engagement — along with snapshot policies, replication, and cloud archive integration (Wasabi, Backblaze) as part of a custom deployment.

How is my storage kept separate from other clients?

Storage shares are provisioned on a per-client basis and access is restricted by VLAN isolation. Only devices on your designated VLAN can access your storage allocation. This logical segmentation is enforced at both the network layer and the storage platform level.

Services & Pricing

What are the three service categories?

- **Hosting:** Rack space, power, cooling, bandwidth, and physical security for client-owned equipment. Clients bring their own servers, workstations, and storage. MelroseINC provides the facility infrastructure and manages the network layer. 3-month minimum commitment.
- **On-Demand Technology:** Monthly access to MelroseINC-owned enterprise equipment — Qumulo storage (per TB), Avid/Mac workstations (per seat), Arista networking (per port), Signiant file transfer, VPN access, and more. 30-day minimum. Scale up or down monthly.
- **Hybrid Integration:** A combination of Hosting and On-Demand, plus integration of public cloud services (Wasabi, Backblaze, LucidLink, Iconik). Most clients use some blend of all three.

What does pricing look like?

PMC pricing is transparent, flat, and inclusive — no egress fees, no overages, no surprise charges. Hosting starts around \$1,000/month for a minimal configuration (2RU server, 1GB bandwidth, network ports). On-Demand starts around \$1,500/month for an entry configuration (2 workstations, 25TB storage, 1GB bandwidth). Comprehensive pricing is always custom-quoted based on actual requirements. All quotes are provided with full itemization.

How does MelroseINC's PMC compare in cost to alternatives?

Consistently less expensive — often significantly so. Skipper Creative, a six-person agency, eliminated over \$30,000 in annual infrastructure costs by moving to our PMC platform while gaining access to enterprise technology they previously couldn't afford. Ignition Creative terminated a real estate lease 18 months early based on PMC savings, and eliminated a \$40,000/year firewall support renewal by moving to our managed firewall service. A current prospect is replacing a five-year-old storage solution — our annual cost for equivalent capacity is less than the vendor's support renewal alone, on a superior, current platform.

Are there any fees not included in the monthly rate?

The only additional fees are one-time onboarding/integration services (clearly quoted in advance), the Premium File Transfer service (\$500 one-time for urgent physical drive ingest), and after-hours labor at premium rates if requested outside standard maintenance windows. There are no data egress fees, no overage charges, and no surprise billing.

Technical Specifications (cont'd)

Support & Service Levels

What are the support tiers?

MelroseINC offers three PMC support levels:

- Standard (On-Demand services and PMC infrastructure): 24x7x365 under a 99.999% uptime SLA with service credits. Covers ISP connectivity, PMC firewalls, switches, and all MelroseINC-provided services.
- Standard Hosting (client-hosted equipment): White-glove hardware support Monday–Friday, 9:00am–6:00pm. Engineer dispatch to facility for troubleshooting, maintenance, parts swaps, LTO tape management, and third-party vendor coordination. 2-hour scheduling response, 4-hour engineer contact.
- Comprehensive Support (optional): 24x7x365 coverage with 4-hour response across all workstations and users, including remote and external users, plus workflow and desktop software support. Purchased for a full workgroup rather than individual users; pricing starts at \$500 per user per month, with custom volume pricing for larger workgroups (20+ users).

What are the response time commitments?

Call intake is 24/7/365. PMC infrastructure and On-Demand services are covered 24x7x365 under the Standard SLA. For Standard Hosting (client-hosted hardware), scheduling response is within 2 hours and engineer contact within 4 hours during business hours (M–F, 9:00am–6:00pm), with on-site dispatch to the PMC facility within 2 hours of a triage decision when on-site support is required. Comprehensive Support provides 24x7x365 coverage with 4-hour response, including after-hours.

What are the maintenance windows?

Routine maintenance is conducted on the 1st and 3rd Monday of each month, from 6:00am to 9:00am, with one-week advance notice provided before each window. Systems may be briefly unavailable during maintenance unless prior arrangements are made. Emergency maintenance outside these windows is performed when required for security patches or critical updates, with notification provided as soon as practicable.

How do I open a support ticket?

Support tickets are opened and managed through a dedicated web-portal which customers are on-boarded to as part of their MelroseINC PMC deployment.

Onboarding & Migration

What does the onboarding process look like?

- Discovery: Assessment call to understand current infrastructure, workflow, team size, and business objectives
- Proposal: Custom quote with full itemization, based on actual requirements — not assumptions
- Proof of Concept (optional): 2-week trial with full access to on-demand services, expert-guided implementation
- Deployment: Professional integration services, white-glove transport for physical equipment if applicable
- Go-Live: Full technical support throughout launch and stabilization period

Most clients are fully operational within two to four weeks of signing.

How is physical equipment transported to PMC?

MelroseINC provides white-glove transport services for clients moving physical equipment to the PMC facility. This service is quoted on a project basis. For initial data migration, clients can drop off physical drives at our MelroseMAC Experience Center in Hollywood for standard transfer (typically completed within 24–48 hours via Signiant), or request a premium same-day transfer service (\$500 one-time) where an engineer personally handles the transfer at the data center.

Technical Specifications (cont'd)

Can we trial MelroseINC's PMC before committing?

Yes. We offer a 2-week Proof of Concept program that gives you full access to on-demand services in a production-equivalent environment. The POC is designed to validate performance, security, and workflow integration before you commit. Our engineering team guides you through the implementation and documents results against your defined success criteria.

How PMC Compares

How is MelroseINC's Private Media Cloud different from public cloud providers (AWS, Azure, Google Cloud)?

- Private infrastructure: Your workloads run on dedicated MelroseINC equipment, not shared multi-tenant public cloud platforms
- No egress fees: Public cloud charges for every gigabyte of data you move out. MelroseINC does not.
- No overages: Public cloud bills escalate unpredictably with usage. Our pricing is predictable and transparent.
- Media-specific: PMC is built for media workflows. Public cloud is general-purpose. Our engineering team speaks your language.
- Physical hardware access: MelroseINC can co-locate your actual workstations and servers. Public cloud cannot.
- Reliability independence: Our infrastructure does not share failure domains with public cloud. When AWS goes down, PMC stays up.

How is PMC different from traditional post-production facilities or server-room MSPs?

- No real estate overhead: Post facilities charge rent-equivalent rates for the space your equipment occupies. MelroseINC's PMC infrastructure pricing includes world-class data center space at a fraction of the cost.
- Enterprise foundation: Most post facilities are not operating to SOC 2, ISO 27001, or the MPA Content Security Best Practices. PMC runs on Equinix's certified foundation and layers its own controls on top.
- Scalability: A server room has fixed capacity. MelroseINC has two full cages today with an expansion path to additional Equinix locations globally.
- No long-term lock-in: Traditional facilities often require long-term leases. MelroseINC requires a 3-month minimum for hosting, then month-to-month.

How is our Private Media Cloud different from companies that just manage their own server room?

- Reliability: An office server room cannot match Equinix-grade power redundancy, cooling, physical security, and 99.999% uptime SLA.
- Cost: When you account for real estate, utilities, hardware refresh, IT staff, and bandwidth, an on-premise server room almost always costs more than PMC — while delivering less.
- Remote work enablement: PMC is built for distributed teams. An office server room ties your workflow to a physical location.
- No capital refresh cycle: Hardware in a server room ages and requires periodic capital investment. MelroseINC absorbs those costs.
- Expertise: MelroseINC provides 100+ years of combined media IT experience. Most companies cannot afford that depth of in-house expertise.

More questions not answered here? Let's connect.

Schedule a discovery call (link to CTA form) or contact us at pmc@melroseinc.com to start the conversation.