SuperSync White Paper

Version: 2.2.0
Date: 2026-04-18

Executive Summary

SuperSync is an enterprise synchronization and realtime data platform for organizations that operate multiple applications, teams, and environments. It provides a single secure control plane for cross-device data synchronization, controlled sharing, and chat-grade realtime delivery, without forcing each product team to build and maintain its own sync stack.

SuperSync is designed for platform engineering groups, SaaS providers, and regulated environments that need consistent security posture, strong tenant boundaries, auditable operations, and predictable deployment behavior. It is built in Go, backed by PostgreSQL for durable metadata, and supports filesystem or S3-compatible object storage for binary payloads.

The Enterprise Problem SuperSync Solves

Large organizations rarely run one product. They run portfolios: operator tools, end-user apps, mobile clients, desktop clients, integration services, and internal automation. Each product needs some form of sync, and each independent sync implementation usually reintroduces the same risks:

- inconsistent identity and authorization behavior
- duplicated security-critical code paths
- weak auditability and unclear operational ownership
- fragmented handling of structured data vs binary content
- poor resilience in realtime workflows and intermittent connectivity

SuperSync addresses this by centralizing sync infrastructure into one hardened, reusable platform.

What SuperSync Delivers

1. A Unified Synchronization Core

SuperSync supports one consistent model across application domains: - structured records and settings - blobs and media metadata - item version history and lifecycle controls - explicit item sharing and revocation - realtime relay and chat workloads

Each application is isolated in its own bucket namespace with capability flags and policy constraints.

2. Strong Tenant and Application Isolation

SuperSync enforces bucket-scoped boundaries by default: - identities are scoped to bucket context - all data operations are authorization-checked per request - feature capabilities are enabled intentionally per bucket - quotas and limits are enforced at bucket and item levels

This model allows multiple products to coexist on one platform while preserving clean security boundaries.

3. Enterprise-Grade Security Defaults

SuperSync security controls are designed as first-class architecture, not add-ons: - Ed25519 challenge-response authentication - short-lived access tokens with refresh-token rotation - strict input decoding and request-size enforcement - rate limiting and abuse visibility - structured audit events and request correlation - quarantine and scanning workflows for uploaded content

4. Realtime and Chat-Ready Transport

SuperSync supports realtime patterns needed by modern collaboration software: - WebSocket endpoints for relay and chat-native flows - SSE and pull APIs for controlled catch-up and fallback - durable message history with cursor-based progression - moderation, access rights, and policy controls for chat channels

This enables both low-latency UX and operationally safe replay/recovery behavior.

Architecture at a Glance

Runtime Components

- `supersyncd`: API server
- `supersync-worker`: background jobs and retention processing
- `supersyncctl`: operational CLI
- `web/portal`: admin and operator-facing UI
- `sdk/go`: typed integration SDK

Storage and Durability Model

- PostgreSQL is the source of truth for metadata, policy state, audit records, and job orchestration.
- Blob content is stored in local disk or S3-compatible object storage.
- Redis is optional for distributed fanout, presence, and rate-limit coordination, but not used as the durable source of truth.

Control Plane and Data Plane

- Data plane: item lifecycle, versioning, sharing, relay/chat payload movement.
- Control plane: auth, bucket/user governance, policy management, auditability, maintenance, and health posture.

Security and Trust Model

Identity and Access

SuperSync uses key-based authentication and bucket-scoped authorization checks for all protected operations. Admin APIs are gated separately by admin credentials.

Encryption Responsibilities

SuperSync is designed for client-side encryption of private payloads: - clients encrypt private data before upload - server stores ciphertext plus metadata required for synchronization - private keys are never stored server-side - sharing uses envelope-style wrapped-key distribution for authorized recipients

SuperSync does not make unsupported "zero-knowledge" claims for metadata and policy surfaces that must remain visible for routing and governance.

Defensive Controls

SuperSync includes practical defense-in-depth controls for production operations: - strict schema validation and unknown-field rejection - replay-resistant auth challenge verification - upload scanning hooks and quarantine support - bounded request and upload guardrails - structured logs with request IDs for incident response

Governance, Compliance, and Operations

SuperSync includes features expected in enterprise operations: - admin dashboard and operational status APIs - audit-event listing and streaming for user and admin scopes - retention and legal-hold controls for chat records - health/readiness/liveness endpoints - Prometheus metrics and tracing hooks - documented backup and restore patterns - deterministic migration workflows for deployment pipelines

Enterprise Use Cases

SuperSync is intentionally domain-agnostic. Typical enterprise workloads include:

1. Cross-device settings synchronization for fleet-managed desktop/server software.
2. Shared metadata and media references for playlist/content platforms.

3. Secure synchronization of connection-manager state and private configuration payloads.
4. Realtime collaboration and messaging channels with governance controls.
5. Notes, revisions, and history synchronization for productivity platforms.

Deployment and Adoption Model

SuperSync is operable by a single platform team and ready for progressive scaling: - local development with Docker Compose - production deployment behind TLS reverse proxy - optional worker separation for background processing - optional distributed runtime features where justified

Organizations can begin with one product bucket and expand to a multi-product portfolio without redesigning auth, storage, or operational controls.

Business Value for Enterprise Buyers

SuperSync reduces platform risk and delivery friction by: - eliminating duplicated sync-stack engineering across products - standardizing security and governance controls across teams - accelerating product delivery with reusable APIs and SDKs - improving operational visibility and audit readiness - creating a stable foundation for future collaboration features

Conclusion

SuperSync is a practical enterprise synchronization platform: security-first, operationally transparent, and extensible across product lines. It provides a shared synchronization substrate that lets engineering organizations invest in product differentiation instead of repeatedly rebuilding critical sync infrastructure.

References

- `README.md`
- `docs/introduction.md`
- `docs/architecture.md`
- `docs/threat-model.md`
- `docs/encryption-model.md`
- `docs/api.md`
- `api/openapi.yaml`