System Architecture

GSCX Platform | Infrastructure & Security Design | April 2026

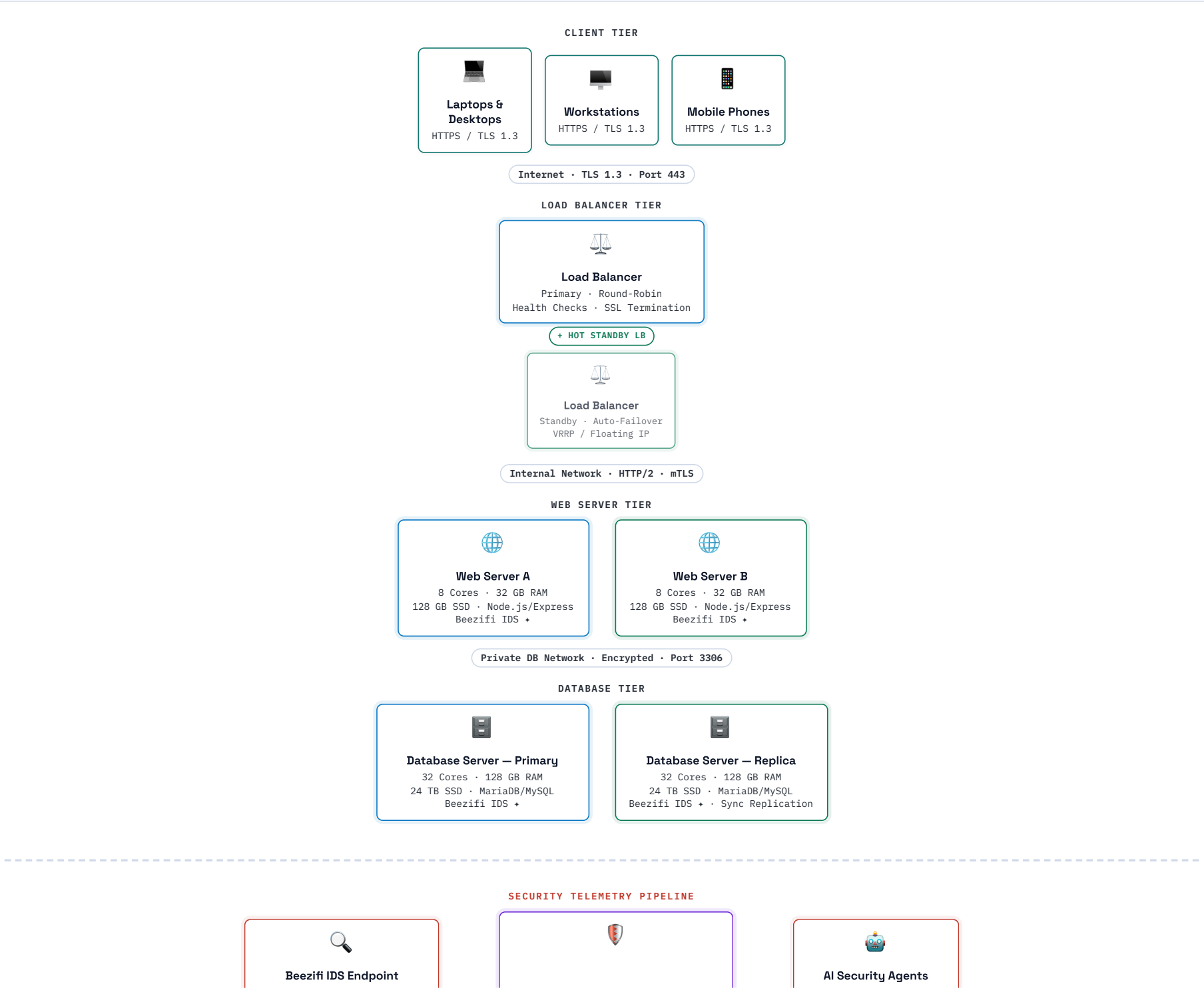
This document describes the full-stack infrastructure of the GSCX platform — a Global Supply Chain Exchange connecting importers, exporters, financiers, logistics providers, insurers, and inspectors across global trade corridors. Coverage spans client endpoints, load balancing, redundant web and database tiers, the integrated Beezifi cybersecurity stack, the GSCX application layer with nine business modules, and four AI copilot services.

ARCHITECTURE PATTERN 3-Tier + Security + AI Overlay	REDUNDANCY MODEL Active / Active with Hot Standby	WEB SERVER NODES 2× (Primary + Standby)	DATABASE NODES 2× (Primary + Replica)	IDS COVERAGE All server nodes
SECURITY OPERATIONS BC3 (Analysts + AI Agents)	APPLICATION MODULES 9 business domains	AI COPILOTS 4 services (Form, Compliance, Recon, Route)	PAYMENT RAILS 6 (SWIFT, ACH, SEPA, WIRE, INTERNAL, CRYPTO)	

> **Design Philosophy:** Every infrastructure layer is deployed with a redundant peer. No single server constitutes a single point of failure. Security telemetry is collected at every node and centralized in BC3 for both automated and human-directed response.

Architecture Diagram

The diagram below illustrates all tiers from client devices through to the database layer and the parallel security telemetry pipeline feeding BC3.


CLIENT TIER
Laptops & Desktops
HTTPS / TLS 1.3
Workstations
HTTPS / TLS 1.3
Mobile Phones
HTTPS / TLS 1.3
Internet · TLS 1.3 · Port 443
LOAD BALANCER TIER
Load Balancer
Primary · Round-Robin
Health Checks · SSL Termination
+ HOT STANDBY LB
Load Balancer
Standby · Auto-Failover
VRRP / Floating IP
Internal Network · HTTP/2 · mTLS
WEB SERVER TIER
Web Server A
8 Cores · 32 GB RAM
128 GB SSD · Node.js/Express
Beezifi IDS ✦
Web Server B
8 Cores · 32 GB RAM
128 GB SSD · Node.js/Express
Beezifi IDS ✦
Private DB Network · Encrypted · Port 3306
DATABASE TIER
Database Server — Primary
32 Cores · 128 GB RAM
24 TB SSD · MariaDB/MySQL
Beezifi IDS ✦
Database Server — Replica
32 Cores · 128 GB RAM
24 TB SSD · MariaDB/MySQL
Beezifi IDS ✦ · Sync Replication
SECURITY TELEMETRY PIPELINE
Beezifi IDS Endpoint
AI Security Agents

✦ **Beezifi IDS** is deployed on every web server and database server node. Telemetry from all nodes streams in real-time to the BC3 Command Center, providing full east-west and north-south visibility.

Traffic Flow

The following steps describe the complete path of a client request from origin to data and back.

1. **Client Request Initiated**
   A laptop, desktop workstation, or mobile phone sends an HTTPS request over TLS 1.3 to the platform's public IP / domain. All client traffic is encrypted in transit — no plain HTTP accepted.

2. **Load Balancer — SSL Termination & Routing**
   The primary Load Balancer terminates TLS, performs IP reputation pre-screening, and forwards the request via round-robin (or least-connections) to an available Web Server node. The hot-standby LB monitors via VRRP and claims the floating IP within seconds should the primary fail.

3. **Beezifi IDS — Inbound Scan (Web Tier)**
   As the request enters the web server, the Beezifi Intrusion Detection software inspects the source IP and payload signature. Flagged IPs are automatically blocked at the host firewall. The source IP is also forwarded to the BC3 telemetry pipeline.

4. **Application Processing (Node.js / Express)**
   The GSCX Express application handles authentication, business logic, and constructs a database query. Session tokens are validated; compliance middleware runs before any data operation. The application serves nine business modules: remittances, import/export orders, transport logistics, cargo insurance, quality inspection, banking & FX, crypto settlement (MooChedda), payment orchestration, and ledger reconciliation. Four AI copilots (Form, Compliance, Reconciliation, Route Advisor) are also available at this tier.

5. **Database Query — Primary Node**
   Queries are directed to the Primary Database Server over the encrypted private DB network. The Beezifi IDS on the DB host monitors all connection attempts and queries for anomalous patterns.

6. **Synchronous Replication to Replica**
   Every write committed to the Primary DB is synchronously replicated to the Replica DB Server before the transaction is acknowledged. This ensures zero data loss on primary failure.

7. **Beezifi IDS — Outbound Scan & Telemetry Dispatch**
   On the response path, the IDS endpoint records the destination IP (client). All captured IP metadata — inbound source and outbound destination — is streamed to the BC3 Command Center for analysis.

8. **BC3 Threat Analysis & Response**
   BC3 receives telemetry from all nodes. AI Security Agents correlate patterns across the fleet in real time. Human security analysts review escalated events. Identified bad actors are proactively blocked across all nodes simultaneously via push-down firewall rules.

9. **Response Returned to Client**
   The web server returns the JSON API response to the load balancer, which re-encrypts with TLS and delivers to the client browser or mobile app.

GSCX Application — Platform Overview

The GSCX application running on the web server tier is a fully-integrated digital exchange for global trade finance. It connects eight specialised member types across the complete lifecycle of cross-border commerce — from product listing and import/export order management through logistics, insurance, inspection, and multi-rail payment settlement — all within a single compliance-enforced platform.

MEMBER ROLES	BUSINESS MODULES	API ENDPOINTS	DATABASE TABLES	PAYMENT RAILS
8 entity types	9 functional domains	120+ REST routes	30 tables	6 rails

AI COPILOTS
4 services

> **Runtime:** Node.js 22 + Express 4 running in PM2 cluster mode (8 workers per node). The application is stateless — sessions are DB-backed, enabling any web server node to handle any request. MariaDB is the single source of truth for all platform data.

Member Role Types

ROLE	PRIMARY FUNCTION	KEY CAPABILITIES
Administrator	Platform governance	KYC/KYB review, OFAC screening, matching engine, reconciliation, compliance flag management
Remitter	Cross-border money transfers	Beneficiary management, multi-rail payout, OFAC screening, purpose code tracking
Importer	Inbound goods management	Import orders, HS code classification, IOR designation, customs workflow, regulatory declarations
Exporter	Outbound goods management	KYB profile, export shipments, ECCN dual-use controls, export license tracking, payout accounts
Transport Provider	Logistics & delivery	Multi-mode shipment tracking, event timeline, customs status, charges & duties, proof of delivery
Insurance Provider	Cargo risk coverage	Quote generation, policy issuance, risk monitoring, claims processing with financial payout
Bank	Financial operations	Account management, multi-rail transactions, FX quotes, compliance flag issuance
Inspector	Quality verification	Inspection reports, photo/video evidence, typed defect classification, payment release gating

Business Modules

The GSCX application is organised into nine functional domains, each backed by dedicated database tables, REST API endpoints, and role-specific user interfaces.

Remittance & Payments

Cross-border money transfers via six payment rails (SWIFT, ACH, SEPA, WIRE, INTERNAL, CRYPTO). Full beneficiary management supporting bank, crypto, and internal recipients. FX quote creation and execution with spread tracking. Every remittance is gated by real-time compliance middleware — BLOCK-severity flags reject the request before processing. Purpose codes, funding sources, and OFAC status tracked per transfer.

Import Order Management

Full inbound goods lifecycle from DRAFT through CUSTOMS_REVIEW to CLEARED or REJECTED. Commercial details (HS codes, quantity, unit price, total value), IOR designation, Incoterms (all 11 terms), shipping mode (AIR/SEA/COURIER/RAIL/ROAD), port of entry, duties payer configuration, and regulatory declarations for FDA, FCC, and USDA requirements. Payment method includes LETTER_OF_CREDIT support. OFAC screening per order.

Export Shipment Management

KYB-verified exporter profile (legal name, tax ID, beneficial owners) with shipment creation covering ECCN dual-use classification, export license number tracking, restricted destination list management, and sanctions confirmation. Status workflow: DRAFT → SUBMITTED → CUSTOMS_REVIEW → SHIPPED → DELIVERED. Payout account assignment for multi-currency proceeds disbursement. Product catalogue with 6 categories, ratings, and certifications.

Transport & Logistics Tracking

Complete logistics record with tracking numbers, AWB/BOL documents, carrier details, and cargo metadata (weight, volume, piece count). Real-time event timeline with 10 event types (LABEL_CREATED, PICKED_UP, IN_TRANSIT, AT_CUSTOMS, CUSTOMS_CLEARED, CUSTOMS_HELD, OUT_FOR_DELIVERY, DELIVERED, EXCEPTION, NOTE). Customs status management (PENDING/CLEARED/HELD/NOT_REQUIRED). Shipment charge management (DUTIES, BROKERAGE, SURCHARGE, DELIVERY_FEE). Full proof-of-delivery capture with recipient name, signature URL, and photo URL.

Cargo Insurance

End-to-end insurance lifecycle from quote generation through policy issuance to claims resolution. Coverage types: ALL_RISK, NAMED_PERILS, TOTAL_LOSS. Quotes carry premium, validity window, and expiry tracking. Policies include certificate URLs, risk level monitoring (LOW/MEDIUM/HIGH/FLAGGED), and coverage date ranges. Claims support incident types (DAMAGE, LOSS, THEFT, DELAY, OTHER), multi-currency invoice and claimed amounts, payout recipient designation (IMPORTER/EXPORTER), and payout status tracking (PENDING → PROCESSING → PAID → DENIED).

Banking & Compliance

Multi-type bank account management (OPERATING, CUSTODIAL, ESCROW, TRUST) with separate available and ledger balance columns for real-time vs. settled tracking. Account status controls (ACTIVE, FROZEN, CLOSED). Transaction processing across all six payment rails with rail-specific metadata (SWIFT message type, ACH SEC code, SEPA scheme). Compliance flag issuance with five flag types, four severity levels, and a full resolution workflow (OPEN → UNDER_REVIEW → RESOLVED/ESCALATED). BLOCK-severity flags halt processing at the middleware layer.

Quality Inspection

Structured inspection reports linked to export shipments, import orders, or transport records. Three result outcomes (PASS, FAIL, CONDITIONAL_PASS) with a workflow status (SCHEDULED → IN_PROGRESS → COMPLETED/FAILED) and an approval signal (APPROVED/FAILED/PENDING) that directly gates payment release. Photo and video evidence upload with timestamped URL storage. Typed defect logging with defect type (COSMETIC/FUNCTIONAL/CRITICAL), severity (LOW/MEDIUM/HIGH/CRITICAL), percentage affected, and recommended action fields.

Crypto Center — MooChedda Integration

Native cryptocurrency settlement available to all members regardless of role. Wallet creation and recovery using secp256k1 / BIP39. Token transfers signed entirely with Node.js built-in `crypto` module — no external signing library. Supports USDC, USDT, BTC, ETH, and any MooChedda-registered token across multiple networks (Ethereum, Solana, TRON). Hosted payment invoice generation with line items, configurable tax, and token preference. Live USDT-denominated market prices. ACH/Wire fiat-to-USDC on-ramp with zero fees. All transfers linked to platform orders for full cross-ledger audit trail.

⚖️ **Payment Orchestration & Reconciliation**

Deterministic cheapest-path route scoring engine evaluates all eligible rails: `baseCost + feeRate × amount + settlementHours × urgencyWeight`. Three urgency tiers (STANDARD 0.5×, EXPRESS 1.5×, URGENT 4.0×). Stores full ranked option set for operations review before execution. Ledger reconciliation runs matching completed platform records against settled bank transactions with three-outcome classification (MATCHED, NO_BANK_TXN, DISCREPANCY) and $0.01 sub-cent tolerance. Admin-controlled bilateral trade matching engine and bond/collateral management with expiry tracking.

AI Platform Services

GSCX ships a pluggable AI platform layer that embeds four intelligent copilots directly into trade finance workflows. A mock heuristic engine runs out-of-the-box; any external LLM is substitutable via the `AI_PROVIDER` environment variable. All jobs are tracked, all outputs stored as scoreable artifacts, and every AI action is audit-logged.

FORM COPILOT
POST /api/ai/form-draft

COMPLIANCE COPILOT
POST /api/ai/compliance/summary

RECONCILIATION COPILOT
POST /api/ai/reconciliation/analyze

ROUTE ADVISOR
POST /api/ai/payment/advise

JOB TRACKING
ai_jobs table (full history)

DOCUMENT RAG INDEX
ai_document_index (chunked)

COPILOT	INPUT	OUTPUT	CONFIDENCE RANGE
Form Copilot	Plain-language trade description (e.g. "send $5k USDC to supplier in Vietnam")	Structured API payload with per-field confidence scores, missing-field highlights, and clarifying questions	0.58 – 0.91
Compliance Copilot	Member ID or transaction reference with active compliance flags	Risk level (LOW–CRITICAL), required documents list, analyst narrative, and prioritised recommended actions	0.70 – 0.95
Reconciliation Copilot	Reconciliation run ID with DISCREPANCY or NO_BANK_TXN entries	Root-cause analysis per entry, suggested matching transactions, and specific resolution steps	0.65 – 0.90
Payment Route Advisor	Payment parameters (amount, currency, recipient type, urgency) and scored route options	Narrative explanation of recommended rail, compliance considerations, corridor risks, and ranked alternatives	0.75 – 0.95

> **Artifact Approval Workflow:** Every AI copilot output is stored as an artifact with a human approval gate (PENDING → APPROVED / REJECTED) before any downstream action is taken. Analyst decisions feed back into the AI models as labelled ground-truth data, continuously improving classification accuracy over time.

Client Tier

The GSCX platform is device-agnostic. All three client categories connect using standard HTTPS (port 443) with TLS 1.3 enforced at the load balancer.

LAPTOPS / NOTEBOOKS	DESKTOP WORKSTATIONS	MOBILE PHONES
Browser-based SPA	Browser-based SPA	Responsive SPA / PWA

Client Security Requirements

- TLS 1.3 minimum — older protocol versions are rejected at the load balancer
- All session tokens stored in `sessionStorage` (not persisted to disk)
- TOTP second factor required for privileged role actions
- No sensitive data cached in browser localStorage

Load Balancer Tier

A redundant load balancer pair sits at the internet edge. The primary node handles all active traffic; the standby node monitors via VRRP heartbeat and assumes the floating public IP within seconds of a detected failure.

TOPOLOGY	PROTOCOL	FAILOVER TIME	TLS TERMINATION	ROUTING ALGORITHM
Active / Hot-Standby	VRRP Failover	< 5 seconds	TLS 1.3 at edge	Round-Robin + Health Check

HEALTH CHECK INTERVAL
5 seconds

Load Balancer Responsibilities

- Terminate inbound TLS; forward to web servers over internal mTLS
- Distribute traffic evenly across Web Server A and Web Server B
- Remove unhealthy web server nodes from the rotation automatically
- Rate-limit excessive connection attempts per source IP
- Forward real client IP via `X-Forwarded-For` header for IDS logging

> **Redundancy Note:** If the primary load balancer fails, the standby node claims the shared virtual IP via VRRP within 2–5 seconds. No manual intervention is required. Clients experience at most one interrupted request during failover.

Web Server Tier

Two identical web server nodes run in an active-active configuration behind the load balancer. Both nodes serve live traffic simultaneously, maximizing throughput and providing immediate redundancy.

Hardware Specification

`CPU: 8 Cores` `RAM: 32 GB` `Storage: 128 GB SSD` `Network: 10 GbE` `OS: Linux (Ubuntu LTS)`

NODE COUNT	RUNTIME	FRAMEWORK	PROCESS MANAGER	SESSION STORAGE
2 (Active-Active)	Node.js (CommonJS)	Express 4.x	PM2 Cluster Mode	Shared (DB-backed)

IDS
Beezifi IDS (on-host)

Web Server Software Stack

COMPONENT	SOFTWARE	ROLE
Application Runtime	`Node.js`	Execute GSCX Express application
Web Framework	`Express 4.x`	REST API routing, middleware pipeline
Process Manager	`PM2`	Cluster mode (8 workers), auto-restart, zero-downtime reload
Reverse Proxy	`Nginx`	Internal TLS termination, static asset cache
Intrusion Detection	`Beezifi IDS`	Real-time IP inspection, automatic blocking, telemetry
Host Firewall	`iptables / nftables`	Enforce blocklist pushed from BC3
Log Shipping	`Filebeat`	Forward access and error logs to BC3 SIEM

Active-Active Redundancy

Both web server nodes run identical application versions at all times. The load balancer performs health checks every 5 seconds against each node's `/api/health` endpoint. If a node fails its health check three consecutive times, it is removed from rotation and the surviving node absorbs all traffic until the failed node recovers.

> **Zero-Downtime Deployments:** PM2 cluster mode enables rolling restarts. The load balancer health check ensures no in-flight requests are terminated during a software update.

Database Server Tier

Two database servers — Primary and Replica — operate in a synchronous replication configuration. Writes go to the Primary; the Replica is promoted automatically on Primary failure. Both nodes run Beezifi IDS for east-west traffic monitoring.

Hardware Specification

`CPU: 32 Cores` `RAM: 128 GB` `Storage: 24 TB SSD` `Network: 25 GbE (DB interconnect)` `OS: Linux (Ubuntu LTS)`

NODE COUNT	DATABASE ENGINE	REPLICATION	RPO (DATA LOSS)	RTO (DOWNTIME)
2 (Primary + Replica)	MariaDB / MySQL	Synchronous (Semi-Sync)	~0 (semi-sync)	< 30 seconds

IDS
Beezifi IDS (on-host)

Database Software Stack

COMPONENT	SOFTWARE	ROLE
Database Engine	`MariaDB 10.x`	Relational data store for all GSCX platform data
Replication	`Semi-Sync Replication`	Writes acknowledged only after replica confirms receipt
HA Orchestration	`Orchestrator / MHA`	Monitors topology, triggers automatic failover
Backup	`Percona XtraBackup`	Hot physical backups — no downtime required
Intrusion Detection	`Beezifi IDS`	Monitor DB connection attempts, query anomalies, lateral movement
Audit Log	`MariaDB Audit Plugin`	Capture all DDL/DML for compliance and forensics

> **Database Isolation:** The database servers are not directly reachable from the internet or the load balancer. Only the web server nodes may connect to the DB tier, enforced by host-based firewall rules and a dedicated private VLAN.

Beezifi Intrusion Detection System

Beezifi IDS is deployed as an on-host agent on every web server and database server node. It provides real-time inspection of all network traffic entering and leaving each host and enforces automatic blocking of identified malicious actors.

Core Capabilities

🔎 **Deep Packet Inspection**

Beezifi IDS inspects all inbound and outbound traffic at the network layer. Signatures for known attack patterns — SQL injection probes, XSS payloads, port scans, brute-force login attempts, and exploit kits — are matched in real time against live traffic streams.

🚫 **Automatic Malicious IP Blocking**

When a source IP is identified as malicious — either by signature match, behavioral anomaly, or threat feed lookup — Beezifi IDS immediately injects a `DROP` rule into the host firewall (`iptables` / `nftables`). No manual intervention required. Blocks take effect in under 100ms.

📡 **IP Telemetry Collection**

Every inbound source IP and outbound destination IP processed by the host is captured by the Beezifi IDS Endpoint and forwarded to the BC3 Command Center over an encrypted telemetry channel. This provides full network visibility for threat hunting and forensic investigation.

🔄 **Threat Feed Integration**

Beezifi IDS continuously syncs with curated threat intelligence feeds (known bad IPs, Tor exit nodes, botnet C2 infrastructure, compromised hosting ranges). Pre-emptive blocks are applied before a connection is even attempted.

Beezifi IDS Endpoint

The Beezifi Intrusion Detection Endpoint is the per-host telemetry agent that bridges on-host detection activity to the centralized BC3 Command Center.

Endpoint Data Pipeline

DATA COLLECTED	DIRECTION	DESTINATION	FREQUENCY
Source IP of every inbound connection	Inbound	BC3 Threat Intelligence	Real-time stream
Destination IP of every outbound connection	Outbound	BC3 Threat Intelligence	Real-time stream
Block events (auto-blocked IPs)	Event	BC3 Incident Queue	Immediate push
Anomaly alerts (behavioral deviation)	Alert	BC3 Analyst Dashboard	Immediate push
Host health metrics (CPU, mem, net)	Health	BC3 Monitoring	Every 30 seconds

> **Endpoint Deployment:** One Beezifi IDS Endpoint agent runs on each of the two web servers and each of the two database servers — four agents total. All four stream to a single BC3 instance, giving security teams a unified cross-node view.

Beezifi Cybersecurity Command Center (BC3)

BC3 is the centralized security operations platform that aggregates telemetry from all Beezifi IDS Endpoint agents across the infrastructure. It provides the tooling, dashboards, and orchestration layer for both human security analysts and AI Security Agents.

BC3 Architecture

INPUT SOURCES	TELEMETRY INGESTION	ANALYST INTERFACE	AI AGENTS	BLOCKLIST PUSH
All IDS Endpoints (×4 nodes)	Real-time streaming	SOC Dashboard + Incident Queue	Automated threat response	All nodes simultaneously

RETENTION
90-day hot / 1-year cold

BC3 Functional Modules

Threat Intelligence Aggregator

Ingests raw IP telemetry from all four Beezifi IDS Endpoint agents. Correlates events across nodes to detect distributed attack campaigns that would be invisible from any single host perspective (e.g., low-rate scans spread across multiple source IPs).

SOC Analyst Dashboard

Provides security analysts with live network maps, alert timelines, IP geolocation overlays, and drill-down incident views. Analysts can manually escalate, suppress, or override automated decisions. All analyst actions are audit-logged.

Blocklist Orchestrator

Maintains a master IP blocklist shared across all server nodes. When BC3 (human or AI) decides to block an IP, the Blocklist Orchestrator pushes the rule to every IDS Endpoint agent simultaneously, ensuring fleet-wide blocking within seconds.

SIEM & Log Archive

All inbound/outbound IP records, block events, and anomaly alerts are indexed and searchable for forensic investigation and compliance reporting. Data is retained for 90 days in hot storage (fast query) and 1 year in cold archival storage.

AI Security Agents

BC3 integrates AI Security Agents that operate autonomously alongside human analysts. These agents continuously analyze telemetry streams, learn from historical patterns, and execute response actions without waiting for human approval — compressing threat response time from minutes to milliseconds.

> **Proactive Posture:** The AI agents are not reactive-only. They build behavioral baselines for every known IP and flag deviations before an attack completes, enabling pre-emptive blocking of bad actors before damage occurs.

AI Agent Capabilities

🧠 **Behavioral Anomaly Detection**

AI agents build statistical models of normal traffic patterns per endpoint, per hour of day, and per user cohort. Deviations — sudden connection spikes, unusual port access, geographic impossibility — trigger automated investigation workflows.

🔗 **Cross-Node Correlation**

A single attacker probing multiple nodes from rotating IPs would evade per-host detection. AI agents correlate timing, payload similarity, and TTL fingerprints across all four server nodes to identify and block coordinated attack campaigns.

⚡ **Autonomous Response Execution**

For high-confidence threat classifications, AI agents push block rules directly through the BC3 Blocklist Orchestrator to all nodes. Lower-confidence findings are escalated to the human analyst queue for review rather than acting autonomously.

📈 **Continuous Learning**

Analyst decisions (confirm block, false-positive override, escalate) feed back into the AI models as labeled ground-truth data. The agents improve their classification accuracy over time, reducing false positives and closing detection gaps.

Human-AI Collaboration Model

THREAT CONFIDENCE	AI ACTION	ANALYST ROLE
`High (>95%)`	Autonomous block pushed to all nodes	Notified; can override within 15 min
`Medium (60–95%)`	Temporary block + escalate to queue	Reviews and confirms or reverses
`Low (<60%)`	Flag and watch; no block	Reviews enriched alert; decides action
`Unknown / Novel`	Capture and sandbox; immediate escalate	Hands-on forensic investigation

Redundancy Strategy

Every tier of the infrastructure is designed with a redundant peer. The following table summarizes redundancy across the full stack.

TIER	PRIMARY	REDUNDANT PEER	FAILOVER MODE	RTO
Load Balancer	LB Primary	LB Hot Standby	VRRP / Floating IP	< 5 sec
Web Server	Web Server A	Web Server B	Active-Active; LB removes failed node	Instant (no failover needed)
Database	DB Primary	DB Replica	Semi-sync replication; auto-promote	< 30 sec
BC3 / IDS	BC3 Primary	BC3 Warm Standby	State sync; manual or auto-promote	< 60 sec

No Single Points of Failure

- **Client connectivity:** Multiple ISP uplinks on the load balancer pair
- **Load balancer:** Hot-standby with shared virtual IP via VRRP
- **Web application:** Two active nodes; either can serve all traffic alone
- **Database writes:** Semi-synchronous replication — replica is always current
- **Database reads:** Can be offloaded to replica during primary maintenance
- **Security monitoring:** BC3 warm standby preserves telemetry continuity

Failover & Recovery Procedures

Load Balancer Failover

1. VRRP keepalive packet is missed by the standby LB (threshold: 3 missed at 1-second interval)
2. Standby LB claims the floating public IP via gratuitous ARP broadcast
3. DNS / BGP upstream sees no change — the IP is the same
4. Traffic resumes through the standby within 2–5 seconds
5. On-call alert fires to the operations team for investigation

Web Server Node Failure

1. Load balancer health check fails three consecutive times against the affected node
2. Node is removed from the active rotation — zero new requests are sent to it
3. Surviving node absorbs 100% of traffic (8 PM2 workers provide ample headroom)
4. PM2 on the failed node attempts automatic process restart
5. Once health check passes, the node is reintroduced to the rotation gracefully

Database Primary Failure

1. Orchestrator detects Primary DB is unreachable (3 consecutive missed heartbeats)
2. Replica is confirmed up-to-date (semi-sync guarantees no data loss)
3. Replica is promoted to Primary — VIP / DNS CNAME updated automatically
4. Web servers reconnect to new Primary using connection pool retry logic
5. A new Replica is provisioned from the promoted Primary to restore HA state

> **Backup Schedule:** Full physical backups via Percona XtraBackup run nightly at 02:00 UTC. Incremental backups run every 4 hours. Backups are stored off-site in a geographically separate location and retained for 30 days.

Hardware Summary

NODE	COUNT	CPU CORES	RAM	STORAGE	ROLE
Load Balancer	2	—	—	—	Traffic routing, TLS termination, HA pair
Web Server	2	8	32 GB	128 GB SSD	Node.js/Express API, SPA serving
Database Server	2	32	128 GB	24 TB SSD	MariaDB Primary + Replica

Software Summary

SOFTWARE	DEPLOYED ON	PURPOSE	STATUS
Node.js / Express	Web Server A, B	GSCX REST API and SPA backend	Active
PM2	Web Server A, B	Cluster process manager, zero-downtime deploys	Active
Nginx	Web Server A, B	Reverse proxy, static asset serving, mTLS	Active
MariaDB	DB Primary, Replica	Relational data store	Active
Beezifi IDS	Web Server A, B · DB Primary, Replica	On-host intrusion detection, auto IP blocking	Security
Beezifi IDS Endpoint	Web Server A, B · DB Primary, Replica	IP telemetry collection, streaming to BC3	Security
BC3 (Beezifi Cybersecurity Command Center)	Dedicated BC3 Server (HA pair)	Centralized threat intelligence, analyst dashboard, AI agents	Command
AI Security Agents	BC3	Automated threat detection, behavioral analysis, autonomous response	Command
Percona XtraBackup	DB Primary, Replica	Hot physical database backups	Ops
Filebeat	All server nodes	Log shipping to BC3 SIEM	Ops
GSCX Application (Node.js/Express)	Web Server A, B	Trade finance platform — remittances, import/export, transport, insurance, banking, crypto, inspection, reconciliation	Active
AI Platform Layer (Copilots)	Web Server A, B	Form Copilot, Compliance Copilot, Reconciliation Copilot, Payment Route Advisor — pluggable provider (mock / LLM)	AI
MooChedda Integration	Web Server A, B	secp256k1 wallet management, USDC/USDT transfers, hosted invoices, live market data — zero external npm dependencies	Active
Multer / KYC Upload Handler	Web Server A, B	KYC/KYB document upload up to 80 MB; admin review and license verification workflow	Ops

> **Security Coverage:** Beezifi IDS and Beezifi IDS Endpoint are deployed on 100% of server nodes. No node in the infrastructure is unmonitored. BC3 provides a single pane of glass across all four server nodes, load balancers, and all telemetry feeds.