Nexa Technologies | Platform Security

Enterprise Security Architecture Program

Cybersecurity Architecture Specification

Nexa Ledger Cloud Platform — Version 4.2

Trust Zones, Threat Model & Compliance Control Mapping

Document ID:	NEXA-SEC-ARCH-2026-014
Classification:	Confidential — Internal Distribution
Version:	3.0 (Approved)
Effective Date:	23 July 2026
Owner:	Platform Security Architecture Team
Review Cycle:	Semi-annual, or upon material architecture change

Prepared by Marcus Chen, Lead Security Architect | Reviewed by Priya Nair, Compliance & Risk | Approved by Elena Kowalski, CISO

Document Control

Revision History

Version	Date	Author	Summary of Changes
1.0	2025-11-04	M. Chen	Initial trust-zone model and STRIDE baseline for Ledger Platform v3.
2.0	2026-03-17	M. Chen	Added multi-region data residency zone; revised IAM section for workload identity federation.
2.1	2026-05-29	P. Nair	Compliance mapping updated for SOC 2 Type II renewal scope.
3.0	2026-07-23	M. Chen	Incorporated risk register heat map; approved for v4.2 release gate.

Approval

Role	Name	Date
Lead Security Architect (Author)	Marcus Chen	2026-07-23
Compliance & Risk Manager (Reviewer)	Priya Nair	2026-07-23
Chief Information Security Officer (Approver)	Elena Kowalski	2026-07-23

1 Executive Summary

This specification defines the security architecture of the **Nexa Ledger Cloud Platform**, a multi-tenant transaction-ledger and reconciliation service operated by Nexa Technologies. It establishes the trust-zone segmentation model, the STRIDE-based threat model for the platform's critical data paths, the identity and access control design, and the mapping of implemented controls against SOC 2 Type II, ISO/IEC 27001:2022, and GDPR Article 32 requirements.

> **Scope.** This document covers the production environment (`ap-south-1` primary, `eu-west-1` secondary) for the Ledger API, the Reconciliation Engine, and the Customer Admin Console. It excludes internal corporate IT systems, which are governed by NEXA-SEC-CORP-2024-002.

Since the v2.0 revision, the architecture has moved from a single flat VPC to a five-zone segmentation model with workload-identity-based service-to-service authentication, closing three of the four Critical findings from the 2026-Q1 penetration test. The remaining Critical finding (unscoped admin session tokens) is tracked as **RISK-014** in Section 7 and is gated for remediation prior to the v4.2 general-availability release.

2 Architecture Overview & Trust Zones

The platform is segmented into five trust zones with monotonically increasing sensitivity. Traffic may only cross a zone boundary through an explicitly enumerated, authenticated gateway; there is no direct routing between non-adjacent zones.

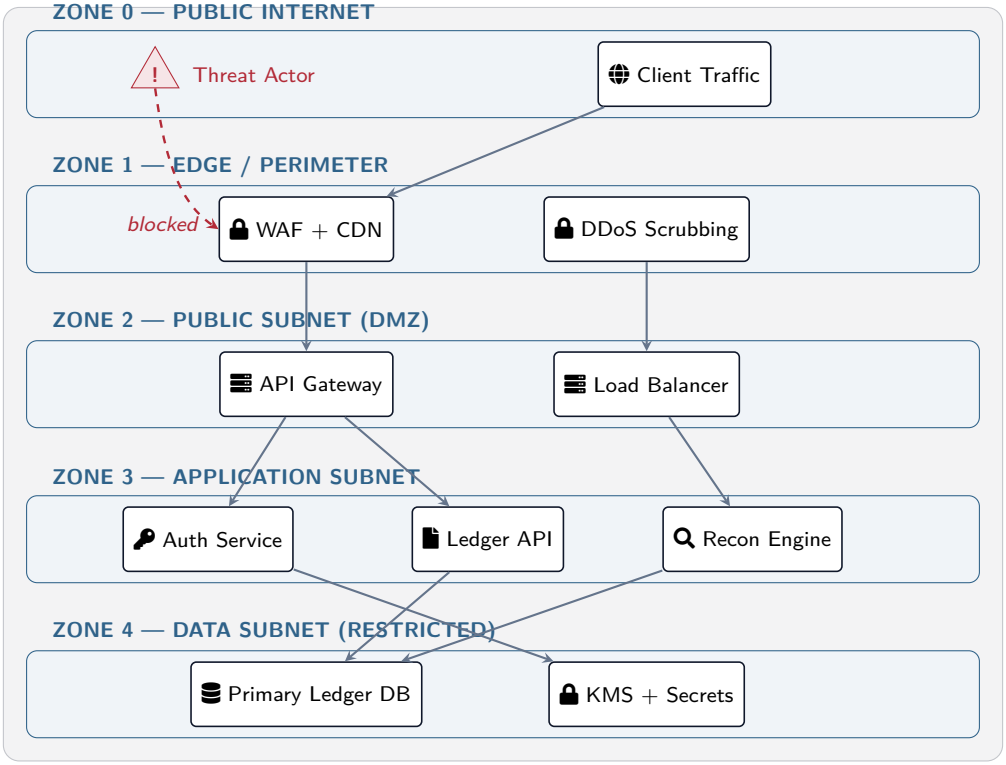

Figure 1. Trust-zone segmentation for the Nexa Ledger Cloud Platform. Each zone boundary enforces mutual TLS and workload-identity authentication; the perimeter blocks unauthenticated lateral movement attempts before they reach the DMZ.

2.1 Zone Boundary Controls

Boundary	Enforced By	Auth Method
Zone 0 → Zone 1	Edge WAF rule sets, geo/IP reputation filtering, rate limiting	TLS 1.3
Zone 1 → Zone 2	Security group allow-list, signed CDN origin headers	mTLS
Zone 2 → Zone 3	Service mesh sidecar policy, JWT audience validation	OAuth2 + mTLS
Zone 3 → Zone 4	Database proxy IAM authentication, VPC endpoint policy	Workload identity

3 Threat Model (STRIDE)

Threats are enumerated per component along the primary transaction path (client → API gateway → ledger service → primary database) using the STRIDE taxonomy. Residual risk reflects likelihood and impact *after* the listed mitigation.

Category	Threat	Mitigation	Residual
Spoofing	Forged service-to-service calls impersonating the Ledger API	Short-lived workload identity certificates (SPIFFE/SVID), mutual TLS on every internal hop	Low
Tampering	Reconciliation batch files altered in transit between Recon Engine and object storage	SHA-256 manifest signing, S3 object lock, append-only audit bucket	Low
Repudiation	Admin disputes having approved a high-value ledger correction	Immutable action log with dual-control approval, signed with per-session key	Low
Information Disclosure	Encryption keys recoverable from a compromised application host	Keys held only in KMS, never materialized on disk; envelope encryption at rest	Medium
Denial of Service	Volumetric flood against the public API Gateway	Edge scrubbing, adaptive rate limiting, autoscaled gateway tier	Medium
Elevation of Privilege	Unscoped admin session token reused across tenant boundaries	*Partial — tenant-scoped claims implemented; console-side enforcement pending (RISK-014)*	Critical

4 Data Classification & Flow

Restricted
: Ledger transaction records, bank account references, KMS key material. Encrypted at rest (AES-256-GCM, envelope encryption) and in transit (TLS 1.3). Access requires just-in-time elevation.

Confidential
: Tenant configuration, reconciliation reports, audit logs. Encrypted at rest; access via role-scoped service accounts only.

Internal
: Aggregated usage metrics, non-identifying telemetry. Standard access controls, no field-level encryption required.

Restricted data flows exclusively within Zones 3–4 and is never written to logs, caches, or the Customer Admin Console's client-side state. Field-level tokenization is applied before any Restricted value leaves the Ledger API's process boundary, including to the Reconciliation Engine, which operates only on tokenized references.

5 Identity & Access Management

Human Access

- SSO via SAML 2.0, enforced hardware-key MFA for all engineering and admin roles.
- Just-in-time production access, 4-hour expiry, approved by second engineer.
- Quarterly access recertification; auto-revoke on role change.

Workload Access

- SPIFFE/SVID identities issued per service, rotated every 24 hours.
- No long-lived static credentials in application configuration.
- Database access brokered through IAM-authenticated proxy; no shared passwords.

6 Compliance Control Mapping

Control ID	Framework(s)	Requirement	Status
AC-02	SOC 2 CC6.1, ISO A.8.2	Least-privilege role assignment, reviewed quarterly	Implemented
CR-05	SOC 2 CC6.7, GDPR Art. 32	Encryption of Restricted data at rest and in transit	Implemented
LG-03	SOC 2 CC7.2, ISO A.8.15	Centralized, tamper-evident audit logging with 400-day retention	Implemented
IR-01	SOC 2 CC7.3, ISO A.5.24	Documented incident response plan with defined severity tiers	Implemented
IAM-09	SOC 2 CC6.3, ISO A.8.5	Tenant-scoped authorization enforced at every access point	Partial
DR-04	GDPR Art. 17, ISO A.5.33	Verified data erasure across all replicas within 30 days	Partial
BC-02	SOC 2 A1.2, ISO A.5.29	Cross-region failover tested at least twice annually	Planned

Audit note. IAM-09's partial status corresponds to RISK-014 (Section 7). The Customer Admin Console currently validates tenant scope server-side on read paths but not yet on the bulk-export path; remediation is scheduled for the 2026-08 sprint ahead of the v4.2 GA gate.

7 Risk Register & Heat Map

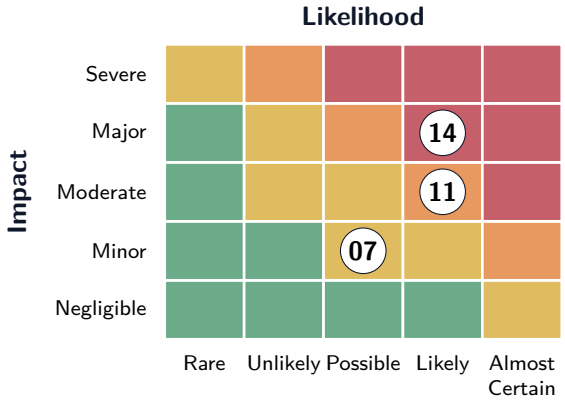

Figure 2. Risk heat map. Circled markers correspond to entries in the risk register below.

ID	Description	Owner	Rating
RISK-007	Reconciliation batch retry storms during upstream bank outage	Recon Platform Team	Medium
RISK-011	Credential-stuffing attempts against tenant admin login	Auth Team	High
RISK-014	Bulk-export path lacks server-side tenant-scope enforcement	Marcus Chen	Critical

8 Monitoring, Logging & Incident Response

All Zone 2–4 components emit structured logs to a centralized, append-only log store with 400-day retention; Restricted-data fields are redacted at the logging shim before transmission. Detection rules cover credential-stuffing patterns, anomalous cross-tenant query volume, and KMS key-usage spikes, each mapped to a PagerDuty severity tier. Confirmed Severity-1 incidents trigger the documented response plan: containment within 30 minutes, tenant notification within 72 hours where GDPR Article 33 applies, and a blameless post-incident review published to the engineering org within five business days.

Approval & Sign-off

This architecture specification is approved for the v4.2 release gate, contingent on remediation of RISK-014 prior to general availability.

Marcus Chen, Lead Security Architect

Elena Kowalski, Chief Information Security Officer