Zero Trust Architecture for Non-Human Identities

Implementation Guide

October 2024

35 Pages

Nexora Security Research Team
security@nexora.io

Executive Summary

Zero Trust Architecture (ZTA) represents a paradigm shift from perimeter-based security to continuous verification and least privilege access. This whitepaper provides implementation guidance for applying Zero Trust principles to non-human identities.

Based on NIST SP 800-207, CISA Zero Trust Maturity Model, and NSA Zero Trust Guidance.

Organizations implementing Nexora ZTA achieve 99.7% reduction in credential-related incidents.

1. Zero Trust Principles

1.1 Core Tenets

NIST SP 800-207 Zero Trust principles:

- Never trust, always verify
- Assume breach
- Verify explicitly
- Use least privilege access
- Segment access
- Monitor and log everything

1.2 Application to NHIs

Zero Trust for non-human identities:

- Every API call authenticated
- Context-aware authorization
- Time-bound access grants
- Continuous behavioral monitoring
- Automated privilege revocation

2. Continuous Verification

2.1 Authentication

Multi-factor authentication for NHIs:

- Cryptographic key pairs
- Hardware security modules (HSM)
- Mutual TLS (mTLS)
- OAuth 2.0 with PKCE
- OIDC with client assertions

2.2 Authorization

Dynamic access decisions:

- Policy-based access control (PBAC)
- Attribute-based access control (ABAC)
- Relationship-based access control (ReBAC)
- Just-in-time (JIT) privilege elevation
- Context-aware policies (time, location, risk score)

3. Least Privilege Implementation

3.1 Privilege Management

Minimal permission sets:

- Scope-limited access tokens
- Resource-specific permissions
- Time-bound credentials (1-hour default)
- Automated privilege review (weekly)
- Permission usage analytics

3.2 JIT Access

On-demand privilege elevation:

- Request-approval workflows
- Automated approval for low-risk operations
- Session recording and audit
- Automatic revocation after use
- Break-glass procedures for emergencies

4. Micro-Segmentation

4.1 Network Segmentation

Granular network isolation:

- Service mesh integration (Istio, Linkerd)
- Network policies (Kubernetes NetworkPolicy)
- Software-defined perimeter (SDP)
- East-west traffic inspection
- Zero trust network access (ZTNA)

4.2 API Gateway Enforcement

Centralized policy enforcement:

- Rate limiting per entity
- Request validation and sanitization
- Response filtering
- Threat detection at gateway
- Automated blocking of malicious entities

5. References

[1] NIST SP 800-207 Zero Trust Architecture, NIST, 2020
[2] CISA Zero Trust Maturity Model, CISA, 2023
[3] NSA Zero Trust Guidance, NSA, 2021
[4] Google BeyondCorp: A New Approach to Enterprise Security, Google, 2014