Hybrid Edge-to-Cloud Zero Trust Security Architecture

Design Overview and Architectural Introduction

Wayne Howlett
Security Architecture • Cloud Security • API Security

Executive Summary

This document provides a **foundational architectural overview** of a **hybrid edge-to-cloud Zero Trust security architecture** designed to enforce network-level access controls, protect sensitive data, and enable secure access across local, cloud, and remote environments. The architecture leverages a **Raspberry Pi 5** as an edge security gateway for DNS-based policy enforcement, combined with **encrypted local storage** and **cloud-native security controls in AWS** to support confidentiality, integrity, availability, and auditability.

The system is designed to operate under **real-world constraints**, including mobility, variable network conditions, and untrusted access environments such as public networks and satellite connectivity. Security controls emphasize **identity-centric access**, **least privilege**, and **defense-in-depth**, with cloud interactions governed through authenticated and authorized API calls and comprehensive audit logging.

This document serves as the **authoritative entry point** for a broader set of security architecture materials. While it establishes architectural intent, scope, assumptions, and design boundaries, **detailed threat modeling, architecture diagrams, control mappings, and implementation evidence are documented in separate supporting documents**. Together, this documentation set demonstrates applied **security architecture, cloud security, and API security practices** suitable for architectural review and professional portfolio presentation.

Introduction

Purpose

This document presents the design, implementation, and validation of a **hybrid security architecture** that integrates **edge-based access control**, **encrypted local storage**, and **cloud-native secure storage** to protect sensitive data and enforce differentiated access policies. The project is intended as a **professional security architecture case study**, demonstrating how modern security principles can be applied in a realistic, resource-constrained environment.

Intended Audience

This document is intended for **security architects, cloud security engineers, and technical reviewers** seeking a high-level architectural overview of the system. It is designed to support architectural reviews, design evaluation, and portfolio assessment, while deferring detailed implementation and configuration specifics to supporting documents.

Project Context

Modern environments increasingly resemble hybrid enterprises, combining on-premises systems, cloud services, mobile access, and untrusted networks. This project treats a residential environment as a **small-scale enterprise security domain**, applying professional security architecture practices to address challenges such as secure remote access, user segmentation, data protection, and policy enforcement under real-world constraints, including mobility and ISP limitations.

A **Raspberry Pi 5** is used as an **edge security gateway**, reflecting deployment patterns common in branch offices, edge computing, and distributed environments. The architecture is intentionally designed to function across multiple network conditions, including traditional ISPs and **Starlink connectivity**, without exposing local infrastructure directly to the internet.

Architectural Overview

The solution follows a **Zero Trust, defense-in-depth approach**, organized across three primary layers:

- **Edge Security Layer**
  Enforces DNS-based access control policies using default-deny rules for restricted devices, explicit allow-listing for approved services, and centralized DNS logging to provide visibility and prevent policy bypass.
- **Secure Storage Layer**
  Protects sensitive local documents using **encryption at rest** and **role-based access control**, ensuring only authorized adult users can access protected data.
- **Cloud Security Layer**
  Implements an encrypted cloud vault in **AWS**, leveraging **S3**, **KMS-managed encryption**, **least-privilege IAM policies**, **multi-factor authentication**, and **CloudTrail audit logging**. All cloud interactions are performed through authenticated and authorized **API calls**, ensuring accountability and traceability across the hybrid environment.

Architecture Domains Covered

The architecture described in this document spans the following security domains:

Security Domain	Coverage
Edge Security	✓
Network Policy Enforcement	✓
Zero Trust Architecture	✓
Cloud Security	✓
API Security	✓
Identity and Access Management	✓
Data Protection	✓
Monitoring and Auditability	✓

Security Architecture Principles

This project is guided by the following principles:

- Zero Trust Architecture (default deny, explicit trust, continuous verification)
- Least Privilege Access Control
- Defense-in-Depth
- Secure Hybrid and Cloud-Native Design
- API-Driven Access Control and Governance
- Auditability and Visibility
- Practical, Risk-Based Decision Making

Development Perspective

The project is informed by the author's **full-stack development background**, enabling security decisions that align with real application, API, and data-flow behaviors. This perspective ensures that security controls are effective, maintainable, and operationally practical rather than theoretical or tool driven.

Document Structure and Scope

This document serves as an **entry point** to a broader set of security architecture materials that collectively describe the system design, implementation, and validation. While the sections outlined here represent the primary focus areas, the architecture and supporting documentation are **intentionally extensible.**

Additional components, refinements, and implementation details may be introduced as the system evolves. Readers are encouraged to refer to the **Contents page** for the most current and complete listing of sections, diagrams, and supporting materials.

Detailed implementation steps, configuration artifacts, command-level instructions, and operational runbooks are intentionally documented in **separate supporting materials.** This document focuses on architectural intent, design boundaries, and security principles, serving as the authoritative entry point for the broader documentation set.

Document Versioning and Change Management

This document set is treated as a **living architecture artifact.** Updates may be made to reflect architectural refinements, security enhancements, implementation changes, or newly identified risks and controls. Significant changes are tracked through versioning and a documented change history.

Assumptions, Scope, and Non-Goals

This section establishes the **architectural boundaries, environmental conditions, and intentional exclusions** that guide the design of the hybrid security architecture. Clearly defining these parameters ensures that security controls are evaluated within a realistic, risk-based context and that architectural decisions remain transparent and defensible.

Assumptions

The architecture is designed based on the following operational and security assumptions:

Operational Assumptions

- The Raspberry Pi edge device is physically secured within a trusted environment and is not accessible to untrusted individuals.
- Local networking equipment (router, access points, switches) is managed and configured by the system owner.
- Internet connectivity may vary in quality and reliability, including mobile and satellite-based connections such as Starlink.
- The system is maintained by a technically proficient administrator responsible for updates, backups, and periodic review of logs.

Security Assumptions

- The home network is not compromised at the time of initial deployment.
- Administrative credentials are protected using strong authentication mechanisms and are not shared.
- End-user devices receive routine operating systems and application updates.
- DNS-based enforcement is a primary control for network access policy, with the understanding that it is part of a layered security approach rather than a single point of defense.
- Cloud services are accessed exclusively through authenticated and authorized API calls governed by least privilege policies.

These assumptions reflect **realistic conditions** for edge and small-scale hybrid deployments and align with common threat models in residential and branch-office environments.

Scope

The scope of this project includes the **architectural design, implementation, and validation** of the following components:

Edge and Network Security

- Deployment of a Raspberry Pi 5 as an edge security gateway.
- Network-level DNS policy enforcement with default-deny behavior for restricted devices.
- Explicit allow-listing for approved services and domains.
- Centralized DNS logging to support monitoring, auditing, and validation of access policies.
- Logical separation between administrative, adult, and restricted devices.

Data Protection

- Secure local storage for sensitive documents using encryption at rest.
- Role-based access control to restrict access to protected data.
- Encrypted backup and storage of critical documents in a cloud-based vault.

Cloud and API Security

- Use of AWS S3 as encrypted cloud storage.
- KMS-managed encryption keys to control data confidentiality.
- Least-privilege IAM policies governing access to cloud resources.
- Multi-factor authentication for administrative cloud access.
- CloudTrail logging to provide visibility into API activity and access events.

Remote Access and Availability

- Secure access to cloud-stored data from untrusted or remote networks.
- No direct exposure of local infrastructure or administrative services to the public internet.
- Support for mobile and remote usage scenarios without degrading security posture.

The project emphasizes **architecture and control design**, focusing on correctness, clarity, and risk management rather than exhaustive feature coverage.

Non-Goals

The following capabilities are intentionally excluded from the scope of this project:

Security Capabilities Not Implemented

- Full endpoint security suites or endpoint detection and response (EDR) across all client devices.
- Deep packet inspection or inline content inspection beyond DNS-based controls.
- Advanced malware analysis, sandboxing, or behavioral analytics.
- Automated incident response orchestration or SOAR platforms.

Enterprise-Scale Features

- Large-scale identity governance and administration (IGA).
- Formal compliance certification (e.g., SOC 2, ISO 27001).
- High-availability clustering, load balancing, or global redundancy.

- Continuous 24/7 SOC monitoring.

Threat Model Limitations

- Defense against highly resourced nation-state or advanced persistent threats.
- Protection against physical compromise of trusted devices by determined attackers.

These exclusions are **intentional architectural decisions** based on risk prioritization, operational complexity, and the intended scope of the system.

Architectural Intent

By explicitly documenting assumptions, scope, and non-goals, this project demonstrates a **risk-aware, architect-driven approach** to security design. Architecture balances confidentiality, integrity, and availability with real-world constraints, while remaining extensible for future enhancements and increased security maturity.

Version Information

Document Title: Hybrid Edge-to-Cloud Zero Trust Security Architecture
Current Version: v1.1
Status: Active – Baseline v1.2
Last Updated: *12/17/2025*

Change Log

Version	Date	Description
v1.0	*12/16/2025*	Initial architecture design and baseline security controls
v1.1	12/17/2025	Assumptions, Scope, and Non-Goals
V1.2	12/17/2025	Added Executive Summary clarifying architectural intent and supporting documentation structure