# Vmobile Enterprise Architecture IT & HR Systems

## Contents

## Version History

| Version | Date | Author | Changes |
|---|---|---|---|
| 1.0 | 1 July 2023 | John D<br>Enterprise Architect | Initial release |
| 1.1 | 2024-04-10 | John D<br>Enterprise Architect | Added SD-WAN segmentation details |
| 1.2 | 2024-09-15 | Martha J<br>Enterprise Architect | Updated endpoint compliance signal exports |
| 1.3 | 2024-11-20 | Rahim K<br>IT Manager | Refined application integration contracts |
| 1.4 | 06/01/2025 | Cook S<br>HR Manager | Workforce & Contractor section update |

## Purpose & Scope

This enterprise architecture establishes the foundational technical, process, and governance standards for Vmobile's HR/IT infrastructure, with a specific focus on integrated telecom operations. The document is designed to guide solution architects, IT operations, security engineering, networking, HRIS platform teams, and facilities management in the design, deployment, and continuous improvement of core systems. It provides authoritative direction on architecture principles, domain models, control planes, segmentation, and telemetry expectations across all major equipment classes and technical domains. This architecture does **not** serve as an end-user configuration guide, operational manual, or reporting artifact; rather, it is a prescriptive reference for enterprise architects and technical stakeholders responsible for system design, integration, and governance.

This document is intended for the following audiences:

- Enterprise Architecture teams responsible for solution design and standards enforcement.
- IT Operations and Security teams managing infrastructure, endpoints, and controls.
- Networking teams overseeing campus, WAN, and cloud interconnects.
- HRIS platform owners and integrators.
- Facilities management overseeing physical access and environmental controls.

Applicability is limited to technical, architectural, and governance stakeholders involved in the planning, implementation, and oversight of Vmobile's HR/IT ecosystem. It is not intended for end users, helpdesk staff, or incident responders seeking operational guidance or troubleshooting procedures.

## Architecture Principles & Domain Model

### Introduction to Guiding Principles for Enterprise Architecture

The Vmobile enterprise architecture blueprint is governed by a set of foundational principles designed to ensure secure, scalable, and resilient operations across all technology domains. These principles are non-negotiable mandates for all architectural decisions and implementations, supporting Vmobile's mission to deliver robust telecom services while upholding regulatory, operational, and business requirements. The domain model outlined herein provides a holistic view of the interconnected domains—Identity, Network, Data, Applications, Endpoints, Observability, Security overlays, and Governance—each of which forms a critical pillar for enterprise-wide IT and HRIS systems. This section articulates the principles and visualizes the domain relationships that inform all subsequent architectural stances and control designs.

## Architecture Principles

- **Zero-Trust Security**
    - All network and application interactions are authenticated and authorized regardless of origin (internal or external). Implicit trust is eliminated; every access request is validated continuously.
    - Impact: Reduces lateral movement risk, enforces strong segmentation, and mandates device and user posture verification at each access attempt.
- **API-First Design**
    - All internal and external integrations are exposed via well-documented, versioned APIs. Service interfaces are standardized and discoverable, enabling modularity and future extensibility.
    - Impact: Accelerates integration, simplifies change management, and supports automation across HRIS, ITSM, and network domains.
- **Observability-by-Default**
    - All systems emit structured logs, metrics, and traces to centralized platforms. Health, performance, and security telemetry are mandatory for endpoints, network devices, applications, and data platforms.
    - Impact: Enables rapid detection of anomalies, supports compliance reporting, and facilitates root-cause analysis for operational incidents.
- **Least Privilege Access**
    - Users, applications, and devices are granted only the minimum access required for their roles and functions. Privileged access is time-bound, auditable, and subject to quarterly recertification.
    - Impact: Minimizes attack surface, reduces risk of privilege escalation, and aligns with regulatory requirements for access control.
- **Data Minimization**
    - Collection, storage, and processing of personal and sensitive data are limited to what is strictly necessary. Data retention policies are enforced, and legal hold mechanisms are integrated with HRIS and ITSM workflows.
    - Impact: Enhances privacy compliance (SOC 2, ISO 27001), reduces regulatory exposure, and streamlines data governance processes.

## Domain Model Overview

The Vmobile enterprise architecture is structured around the following core domains, each with explicit boundaries and integration points:

- **Identity**
    - Centralized workforce and contractor identity sources; lifecycle management (JML); SSO/MFA trust flows; privileged access and hardware authenticators.
- **Network**
    - SD-WAN edges, campus LAN/WLAN, data center/cloud interconnects; segmentation and microsegmentation; perimeter controls.
- **Data**
    - Ingest pipelines, storage layers (lake/warehouse), governance, lineage, retention, and security overlays.
- **Applications**
    - HRIS, ITSM, CRM, ERP, and supporting business applications; integration contracts via REST/eventing; interface governance.
- **Endpoints**
    - Managed laptops, desktops, mobile devices, conference room A/V, badge readers, network CPE, and accessories; compliance signal export and device management.
- **Observability**
    - Central telemetry (logs, metrics, traces), SIEM/SOAR orchestration, device and application health streams.
- **Security Overlays**
    - Defense-in-depth controls, NGFW rules, endpoint protection (EDR/MDM), DLP, artifact signing, and SBOM scanning.
- **Governance**
    - Policy enforcement, compliance mapping (SOC 2/ISO 27001), privacy alignment, and physical security integration.

## Identity & Access (High-Level)

The Identity & Access domain serves as the authoritative foundation for workforce and contractor authentication, authorization, and lifecycle management across Vmobile’s enterprise landscape. This section outlines the architectural approach to identity sources, lifecycle events, trust flows, privileged access, and the integration of device and hardware authenticators. All guidance is at the enterprise architecture and control plane level; end-user configuration instructions and password specifics are explicitly excluded (see Non-Overlap list).

### Workforce & Contractor Identity Sources

Authoritative identity sources underpin all access and control decisions within the organization. Vmobile employs a multi-source identity model, anchored by the HRIS for employees and a contractor management system for non-employees. The Joiner-Mover-Leaver (JML) lifecycle is strictly enforced, ensuring timely provisioning, modification, and deprovisioning of access.

Identity is established at onboarding ("Joiner"), updated for role changes or transfers ("Mover"), and systematically revoked at termination or contract end ("Leaver"). Integration between HRIS, contractor management, and IAM platforms is automated via SCIM and API connectors, with event-driven updates to downstream systems.

### Identity Type to Source System Mapping

| Identity Type | Source System | JML Lifecycle Events |
|---|---|---|
| Employee | HRIS (e.g., Workday) | Joiner, Mover, Leaver |
| Contractor | Contractor Mgmt Portal | Joiner, Mover, Leaver |
| Privileged Admin | HRIS + IAM (Okta) | Joiner, Mover, Recertify |
| Service Account | IAM (Okta, Vault) | Create, Rotate, Decommission |

## Trust Flows & Privileged Access

Enterprise trust flows are standardized via Single Sign-On (SSO) and Multi-Factor Authentication (MFA), with Okta as the central identity provider. All workforce and contractor identities are federated through Okta, enforcing MFA for all access to Tier 1 and Tier 2 applications. Device posture is factored into authentication, leveraging endpoint compliance signals for conditional access.

Privileged access is tightly controlled through Just-In-Time (JIT) elevation, quarterly access recertifications, and secrets management protocols. Administrative privileges are granted only as needed, with automatic expiry and mandatory review cycles.

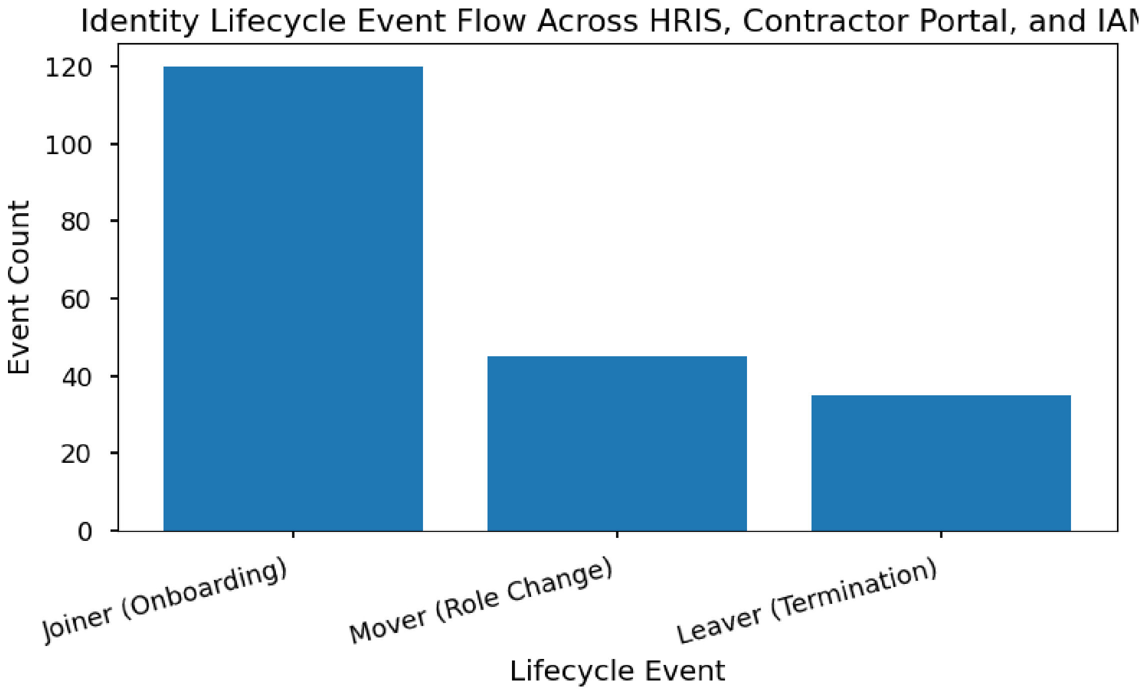
### Privileged Access Control List

- Just-In-Time (JIT) access elevation for admins and operators.
- Quarterly privileged access recertification and attestation.
- Centralized secrets management (Vault integration).
- Enforced MFA for all privileged operations.
- Hardware-backed authentication for elevated roles.

## Device & Hardware Authenticators

Hardware authenticators, including FIDO2 security keys, are architecturally mandated as part of the device and identity trust model. These authenticators provide phishing-resistant, non-repudiable access for workforce and privileged users. Device trust is established via endpoint compliance checks (MDM/EDR signals), with hardware authenticators serving as a prerequisite for privileged access and sensitive workflows.

The architectural stance is to require hardware-backed authentication for all Tier 1 system access, with integration into Okta's device trust framework. Device registration is automated during onboarding, with regular attestation of hardware status and compliance exported to IAM systems.

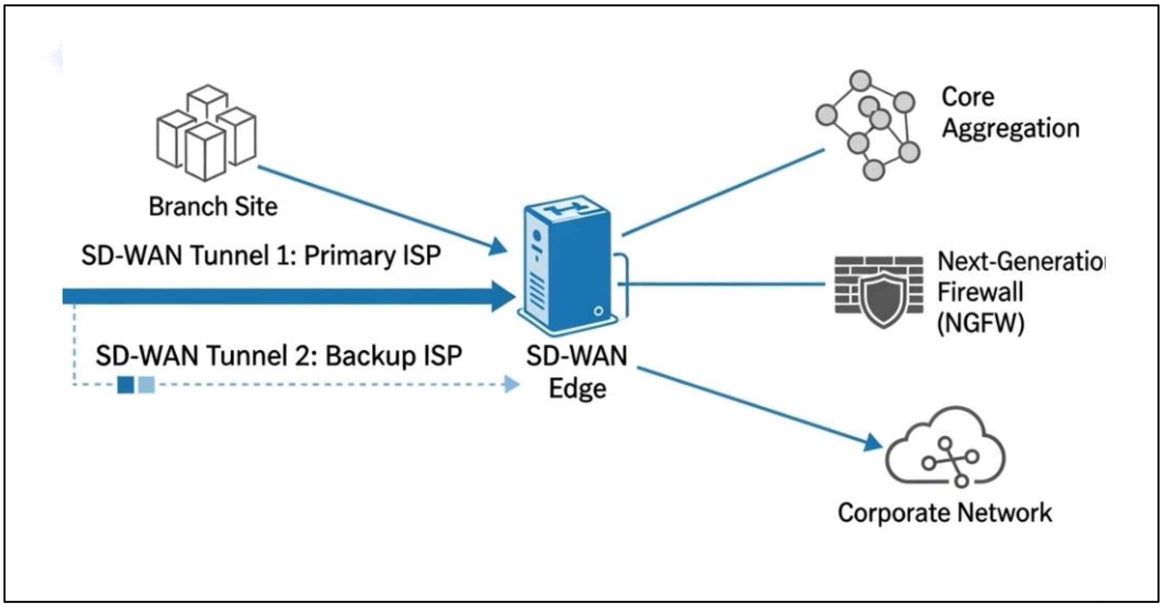


## Network Architecture (SD-WAN, Campus, DC/Cloud)

The Vmobile enterprise network architecture is structured across multiple domains to ensure secure, performant, and resilient connectivity for all business-critical services. The architecture spans wide-area networking (WAN) via SD-WAN, campus LAN/WLAN, data center (DC) and cloud interconnects, and enforces rigorous segmentation at every layer. Segmentation is foundational—enabling least privilege, reducing lateral movement risk, and supporting compliance requirements. All network design aligns to zero-trust principles, with identity-driven access controls and observability integrated by default.

### WAN & SD-WAN Edges

The WAN topology leverages SD-WAN edge appliances deployed at each branch site, Network Operations Center (NOC), and major office. Each SD-WAN edge is provisioned with dual uplinks (primary and backup) to maximize availability and support application-aware routing. Traffic policies are centrally orchestrated to prioritize critical enterprise applications, optimize bandwidth usage, and enforce security overlays. SD-WAN tunnels terminate at core aggregation points, with traffic inspected at next-generation firewalls (NGFW) before entering the protected network zones.


Branch Site
SD-WAN Tunnel 1: Primary ISP
SD-WAN Tunnel 2: Backup ISP
SD-WAN Edge
Core Aggregation
Next-Generatio Firewall (NGFW)
Corporate Network

## Campus LAN/WLAN

The campus network is architected with a Layer 3 (L3) core and Layer 2 (L2) access switches, supporting high availability and simplified routing domains. Wi-Fi infrastructure is built on enterprise-grade access points managed by centralized controllers. SSID segmentation is strictly enforced: corporate SSIDs are mapped to secure VLANs with full identity-based authentication (802.1X, EAP-TLS), while guest SSIDs are isolated to DMZ VLANs with restricted internet-only access. Access controls are policy-driven and monitored for anomalous device behaviors.

### Guest vs Corporate SSID Segmentation and Access Controls

| SSID Type | VLAN Assignment | Authentication Method | Network Access Scope | Internet Access | Device Isolation | Monitoring & Logging | Policy Enforcement |
|---|---|---|---|---|---|---|---|
| Corporate | Secure VLAN | 802.1X (EAP-TLS) | Full enterprise resource | Yes | No | Full (SIEM, NAC integration) | Strict (NAC, NGFW) |
| Guest | DMZ VLAN | Captive Portal | Internet only | Yes | Yes | Basic (DHCP, portal logs) | Rate limiting, egress FW |
| Restricted | Dedicate | 802.1X | Specific | No | Yes | Enhance | Whitelist |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | d VLAN | (EAP-TLS) | app/resource | | | d (access logs) | only |
| Management | Mgmt VLAN | MAC auth + SSO | Network equipment only | No | Yes | Full (admin actions) | Role-based, NGFW |

### Data Center & Cloud Interconnect

Within the data center, the network follows a spine/leaf architecture for optimal east-west scalability and low-latency connectivity between compute clusters and storage arrays (SAN/NAS). Management networks and out-of-band paths are physically and logically separated. Cloud interconnects are established via private peering links, leveraging direct connect or express route technologies for secure, high-throughput data exchange. All interconnects are subject to identity-based access controls and continuous telemetry.

### Segmentation Model

- **User Segmentation:** Individual user devices are assigned to dedicated VLANs or overlay segments based on identity, role, and compliance posture.
- **Corporate Segmentation:** Core business applications and services reside in protected network zones, accessible only via authenticated and authorized endpoints.
- **Restricted Segmentation:** Highly sensitive resources (e.g., HRIS, financial systems) are isolated within restricted segments, accessible only to explicitly whitelisted identities.
- **Management Segmentation:** Network management plane traffic (device admin, monitoring) is confined to management VLANs, with access granted solely to privileged IT staff and automation systems.
- **Guest Segmentation:** Untrusted devices (visitors, contractors) are placed on guest VLANs with strict egress controls and no access to internal resources.
- **Microsegmentation:** East-west traffic within data centers and cloud environments is segmented at the workload or application level, minimizing lateral movement and enforcing granular policy controls.

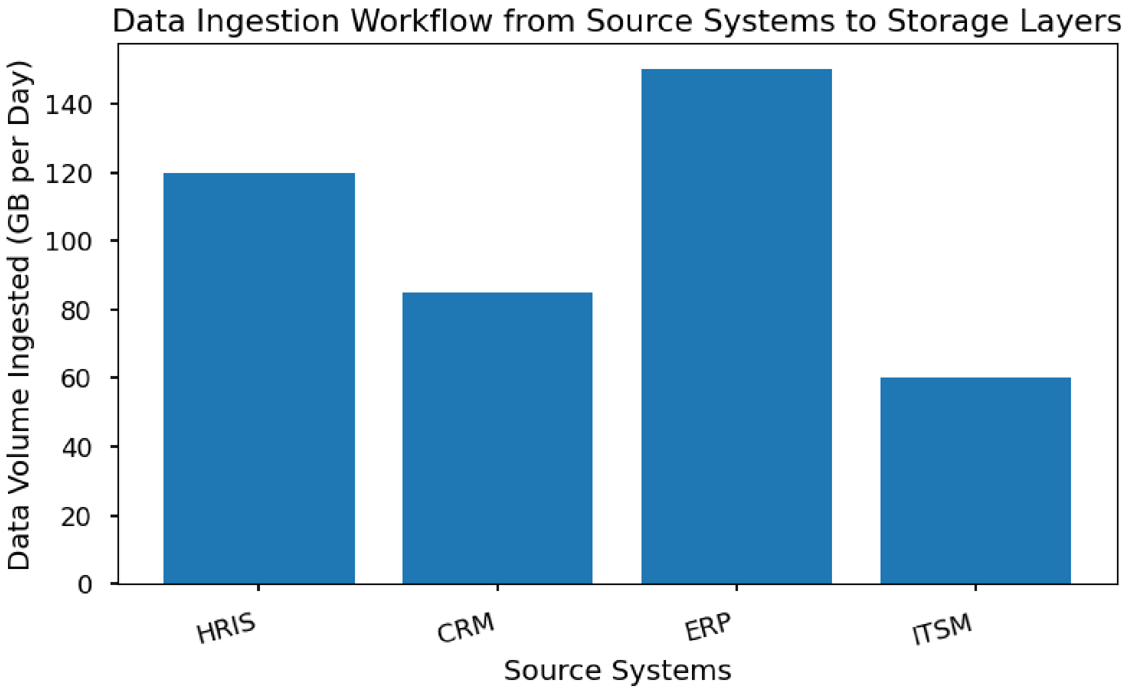
## Data Platform (Ingest, Storage, Governance, Lineage)

The Vmobile Enterprise Data Platform is architected to support secure, scalable, and governed data flows across all major business domains, including HRIS, CRM, ERP, and ITSM. The platform is designed for high-volume, high-velocity data ingestion, robust storage tiering, and comprehensive lineage tracking, with strict adherence to regulatory and internal governance requirements. This blueprint outlines the architectural stance for data ingest, storage layers, cataloging, security controls, retention, and legal hold mechanisms. End-user configuration guides and reporting playbooks are explicitly excluded; refer to the Non-Overlap list for those resources.

## Data Ingest & ELT Patterns

Data ingestion into the Vmobile Data Platform is facilitated via both streaming and batch ELT (Extract, Load, Transform) connectors. Streaming connectors are leveraged for real-time event capture from systems such as ITSM and CRM, supporting immediate operational analytics and alerting. Batch ELT connectors are employed for periodic synchronization from HRIS and ERP, optimizing throughput for large, structured datasets.

- **Streaming ELT:** Utilizes event-driven frameworks for low-latency ingestion, schema enforcement, and real-time lineage.
- **Batch ELT:** Scheduled jobs extract data at defined intervals, transforming and loading into storage layers with full audit trails.
- **Source Systems:** HRIS (Workforce data), CRM (Customer interactions), ERP (Financials), ITSM (Incident and asset data).



### Storage Layers & Catalog

The platform adheres to a tiered storage architecture, enabling progressive refinement and governance of data assets. Cataloging is enforced at each layer, with sensitivity labels and lineage metadata attached for compliance and operational clarity.

| Layer | Description | Cataloging Practices |
|---|---|---|
| Bronze | Raw, unprocessed ingested data | Auto-registration, basic metadata |
| Silver | Cleansed, conformed, and lightly transformed | Enriched metadata, sensitivity labeling |
| Gold | Fully curated, business-ready datasets | Full lineage, access controls enforced |

### Security, Retention & Legal Hold

- **Row/Column Security Controls:**
  - Attribute-based access controls (ABAC) for sensitive fields.
  - Masking of PII data at query and export layers.
  - Segregation of access by domain and role.
- **Retention Policies:**
  - Automated data lifecycle management per regulatory requirements.
  - Configurable retention windows per data class (e.g., HR, finance).
  - Legal hold triggers on data subject to investigation or litigation.
- **Legal Hold Mechanisms:**
  - Immutable storage for held datasets.
  - Auditable access logs for held data.
  - Integration with compliance workflows for release and review.

This architecture ensures that all data ingested, stored, and processed within the Vmobile ecosystem is governed, secure, and compliant with enterprise and regulatory standards.

## Application Integration (Contracts & Patterns)

Enterprise application integration at Vmobile adheres to rigorous architectural patterns designed to enable secure, reliable, and scalable interoperability across core business platforms. This blueprint governs integration between HRIS, IAM, ITSM, Data Platforms, and other enterprise systems, leveraging standardized protocols and contracts to ensure consistency, auditability, and future extensibility. All integration approaches are aligned with the principles of API-first development, observability-by-default, and least privilege, with explicit controls for versioning, error handling, and authentication.

Integration is not end-user configuration or troubleshooting guidance; it is the technical foundation for secure, automated, and maintainable inter-system communication. End-user guides and training decks are referenced elsewhere and not included here.

## REST vs Eventing

RESTful APIs and event-driven architectures represent the two primary integration patterns in Vmobile's enterprise architecture. RESTful APIs offer synchronous, request/response interactions suitable for transactional workflows, while event-driven patterns (via enterprise event buses and schema registries) enable asynchronous, decoupled communication for scalable, real-time data propagation.

Both patterns are governed by strict interface contracts, including OpenAPI specifications, versioning policies, standardized error models, and robust authentication/authorization mechanisms (OIDC/SAML). Idempotency and correlation IDs are mandated to ensure reliability and traceability. Dead Letter Queues (DLQs) and exponential backoff strategies are required for eventing to handle failure scenarios gracefully.

The following table summarizes key feature comparisons:

| **Feature** | **RESTful API Integration** | **Event-Driven Integration** |
|---|---|---|
| Versioning | URI-based (e.g., /v1/resource), OpenAPI spec; must support backward compatibility | Schema registry; event versioning via metadata; consumers must handle schema evolution |
| Error Model | Standardized HTTP status codes (4xx/5xx); error payloads with codes/messages; retry guidance in contract | Event NACKs, DLQ routing, error events with structured payloads; consumer-side retry/backoff |
| Idempotency | Required for POST/PUT; Idempotency-Key header enforced; contract specifies idempotent operations | Event deduplication via event IDs; consumer must handle repeated delivery gracefully |
| Authentication | OIDC/SAML tokens; scopes per endpoint; least privilege enforced | Event bus ACLs; producer/consumer authentication via service identity; topic-level permissions |
| Correlation | Correlation-ID header for tracing across requests; required in all contracts | Event metadata includes correlation IDs; enables end-to-end traceability |
| Observability | Structured logging for requests/responses; metrics | Event delivery metrics; trace propagation via event |

| | | |
|---|---|---|
| | (RED); distributed tracing integrated | metadata; centralized event audit logs |
| Error Recovery | Contract defines retry logic, backoff, and escalation paths | DLQ for failed events; automated reprocessing; alerting on event delivery failures |
| Interface Definition | OpenAPI/Swagger; explicit contract published and versioned | Avro/Protobuf schemas; registry of event contracts; versioned and discoverable |
| Use Cases | HRIS↔IAM attribute sync, transactional updates | ITSM↔Data platform notifications, HRIS onboarding events, security alert propagation |

## Interface Contracts

The following are selected examples of interface contracts governing integration between critical enterprise systems:

- **HRIS ↔ IAM (Identity Attribute Sync):**
  - RESTful API contract for periodic and event-driven sync of workforce identity attributes (e.g., name, email, role, department) from HRIS to IAM.
  - OpenAPI definition specifying required fields, authentication scopes, error handling, and idempotency requirements.
  - SCIM protocol support for bulk provisioning and deprovisioning.
  - Event contract for onboarding/offboarding triggers, including correlation IDs and status events.
- **ITSM ↔ Data Platform (Incident Data Ingest):**
  - Event-driven contract for publishing ITSM incident creation, update, and resolution events to the Data Platform.
  - Schema registry for incident event payloads, including fields for ticket ID, priority, timestamps, and affected assets.
  - DLQ routing for failed event processing; consumer-side retry logic mandated.
  - REST API for querying incident history and status, with explicit versioning and error model.
- **HRIS ↔ IAM (Access Request Workflow):**
  - REST API contract for submitting and approving access requests initiated from HRIS to IAM.
  - Explicit definition of request/approval payloads, authentication requirements, and audit logging.
  - Event notification contract for status changes (approved, rejected, escalated).

- **ITSM ↔ Data Platform (Asset Change Events):**
  - Event bus contract for publishing asset lifecycle changes (add, update, retire) from ITSM to the Data Platform.
  - Schema evolution policy and consumer compatibility requirements.
  - Correlation ID inclusion for traceability across systems.
- **HRIS ↔ IAM (JML Lifecycle Eventing):**
  - Event contract for Joiner, Mover, Leaver (JML) lifecycle events emitted by HRIS and consumed by IAM for automated provisioning/deprovisioning.
  - Structured payloads with required fields, status codes, and error recovery logic.
- **ITSM ↔ Data Platform (Compliance Signal Sync):**
  - REST API contract for periodic sync of compliance signals (patch status, encryption state) from ITSM endpoint management to Data Platform for reporting and analytics.
  - Explicit contract for authentication, data retention, and error handling.

All interface contracts are subject to quarterly review and must be published in the central contract registry. Integration patterns are standardized to ensure interoperability, auditability, and security across Vmobile's enterprise platforms.

## Endpoint & Device Management (MDM/EDR Signals; Rings; BYOD)

Effective endpoint and device management is foundational to Vmobile's enterprise architecture, ensuring operational integrity, security, and compliance across all IT and HRIS-managed assets. This section explicitly enumerates each endpoint class under management, articulates the architectural stance for control, segmentation, and telemetry, and details compliance signal flows and software delivery mechanisms. All device classes, whether user-facing or infrastructure, are managed under robust policy frameworks, leveraging MDM (Mobile Device Management), EDR (Endpoint Detection and Response), and integration with IAM (Identity & Access Management) systems. No end-user configuration steps or inventory listings are included; this blueprint is strictly architectural in scope.

### Endpoint Classes

Below is the explicit enumeration of endpoint equipment classes covered in the Vmobile environment. For each, architectural stance, segmentation, and telemetry expectations are stated.

- **Laptops**
  - Corporate-issued Windows/macOS devices, managed via MDM/EDR.
  - Segmented into user/corporate/restricted zones.

  - Device posture signals (encryption, patch status, EDR agent) exported to IAM for access gating.
  - Software delivery via enterprise catalog; admin-on-demand privilege elevation.
- **Desktops**
  - Fixed workstations, managed identically to laptops.
  - Segmentation mirrors laptop policy, with additional controls for shared-use stations.
  - Telemetry includes hardware health and compliance signals.
- **Monitors**
  - Managed as accessories; asset registration required for high-value models.
  - No direct compliance signals, but included in physical asset tracking.
- **Printers**
  - Networked (IPPS/IPP) and USB-attached models.
  - Segmentation: restricted to print VLANs; access controlled via IAM.
  - Telemetry: print job logging, device health.
- **Mobile Phones & SIMs**
  - Corporate-issued and BYOD boundary enforced via MDM enrollment.
  - Policy enforcement: encryption, screen lock, patch currency.
  - SIM management: corporate SIMs tracked; BYOD SIMs excluded from core network access.
- **Docks, Adapters, Cables (USB-C/HDMI)**
  - Managed accessories; asset control policies apply to enterprise-issued items.
  - Device trust extended only to docked devices meeting compliance signals.
- **Conference Room A/V Systems**
  - Teams Room systems, cameras, table microphones, speakers/soundbars, touch panels/controllers, whiteboard cameras, in-room PCs, room scheduling panels.
  - Segmentation: dedicated A/V VLANs; management path isolated from media path.
  - Telemetry: device health, firmware compliance, room utilization metrics.
- **Badge Readers/Biometric Devices**
  - Used for facilities and data center access.
  - Segmentation: restricted management network; physical access logs exported to SIEM.
  - Telemetry: access event logging, device status.
- **Network CPE & Branch Gear**
  - SD-WAN edges, switches, routers, firewalls.
  - Segmentation: management, user, guest, and restricted zones.
  - Telemetry: device health, configuration drift, compliance signals.

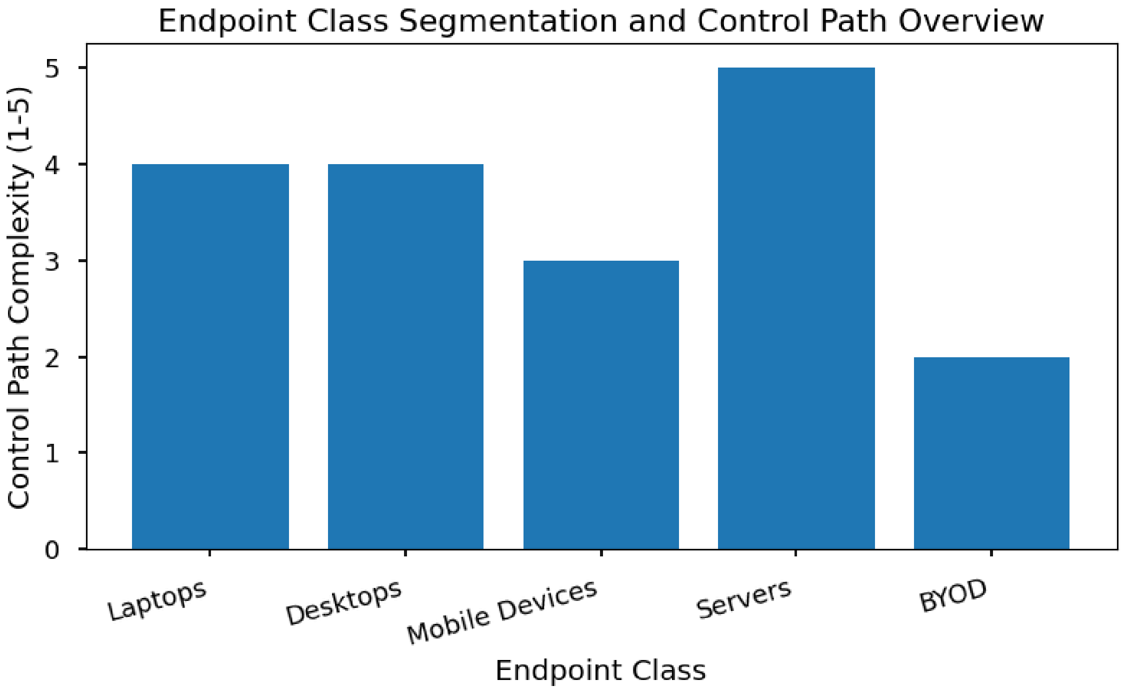
- *See Section 5 for network architecture details.*

## Compliance Signals & Software Delivery

All managed endpoint classes export compliance signals—such as encryption state, patch currency, EDR status, and firewall posture—to the IAM platform, enabling dynamic access control and privileged operation gating. Software delivery is orchestrated via the enterprise application catalog, with admin-on-demand workflows for privilege elevation, ensuring least-privilege operation across the fleet. Compliance signals are collected via MDM/EDR agents and forwarded to central policy engines for continuous evaluation.

### Endpoint Class Compliance Signal Mapping

| Endpoint Class | Compliance Signals Exported | Control Plane |
|---|---|---|
| Laptops | encryption, Patch Status, EDR, Firewall | MDM/EDR, IAM |
| Desktops | Encryption, Patch Status, EDR, Firewall | MDM/EDR, IAM |
| Monitors | Asset Registration | Asset Management |
| Printers | Print Logs, Device Health | Print Server, IAM |
| Mobile Phones & SIMs | Encryption, Patch Status, Screen Lock | MDM, IAM |
| Docks/Adapters/Cables | Asset Registration | Asset Management |
| Conference Room A/V Systems | Firmware Status, Device Health | A/V Management, SIEM |
| Badge Readers/Biometric Devices | Access Logs, Device Status | Physical Access Mgmt, SIEM |
| Network CPE & Branch Gear | Config Drift, Device Health, Compliance | Network Mgmt, SIEM |



All compliance and telemetry flows are architected for observability-by-default, supporting rapid detection and remediation of non-compliance or anomalous device behavior. Software delivery via catalog is strictly managed; no direct installation by end-users outside approved workflows.

## Observability & Telemetry (Logs/Metrics/Traces; SIEM/SOAR)

Observability and telemetry are foundational pillars of Vmobile's enterprise architecture, enabling proactive monitoring, rapid incident response, and continuous improvement across all IT domains. This blueprint prescribes a unified observability model encompassing structured logging, metrics, distributed tracing, and automated security orchestration. All equipment classes—including endpoints, room A/V systems, network infrastructure, and data center hardware—must emit standardized telemetry signals to central platforms for real-time analysis and compliance enforcement. Integration with SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) ensures that identity, network, and application anomalies are detected, correlated, and remediated in accordance with enterprise policy.

### Logging & Metrics

Structured logging is mandated across all critical flows, including authentication (SSO/MFA), HRIS transactions, ITSM operations, and device management events. Logs must conform to a standardized schema with timestamp, identity, device posture, and transaction context. Metrics collection follows RED (Rate, Errors, Duration) and USE (Utilization, Saturation, Errors) models for service endpoints, network devices, and room A/V systems. Distributed tracing is enforced for authentication flows and cross-domain integrations, enabling root cause analysis and performance optimization.

### SIEM/SOAR Integration

- Identity anomaly detection (e.g., impossible travel, privilege escalation attempts)
- Network segmentation violations (e.g., unauthorized lateral movement)
- Endpoint compliance failures (e.g., missing encryption, outdated EDR signatures)
- Room A/V health monitoring (e.g., offline controllers, failed firmware updates)
- Automated containment orchestration (e.g., isolate device, revoke session)
- Incident enrichment with device posture and user context
- Alert forwarding to SOC for manual escalation
- Integration with IAM for automated access revocation

## Non-Functional Requirements (Targets)

The Vmobile enterprise architecture is underpinned by robust non-functional requirements that ensure reliability, performance, scalability, and resilience across all IT and HR systems. These requirements are foundational for supporting mission-critical telecom operations and HRIS processes. This section defines the architectural targets for availability, performance, and scalability, and outlines resilience principles and recovery objectives. These standards apply across all equipment classes, network domains, and application platforms referenced in previous sections.

### Availability & Performance

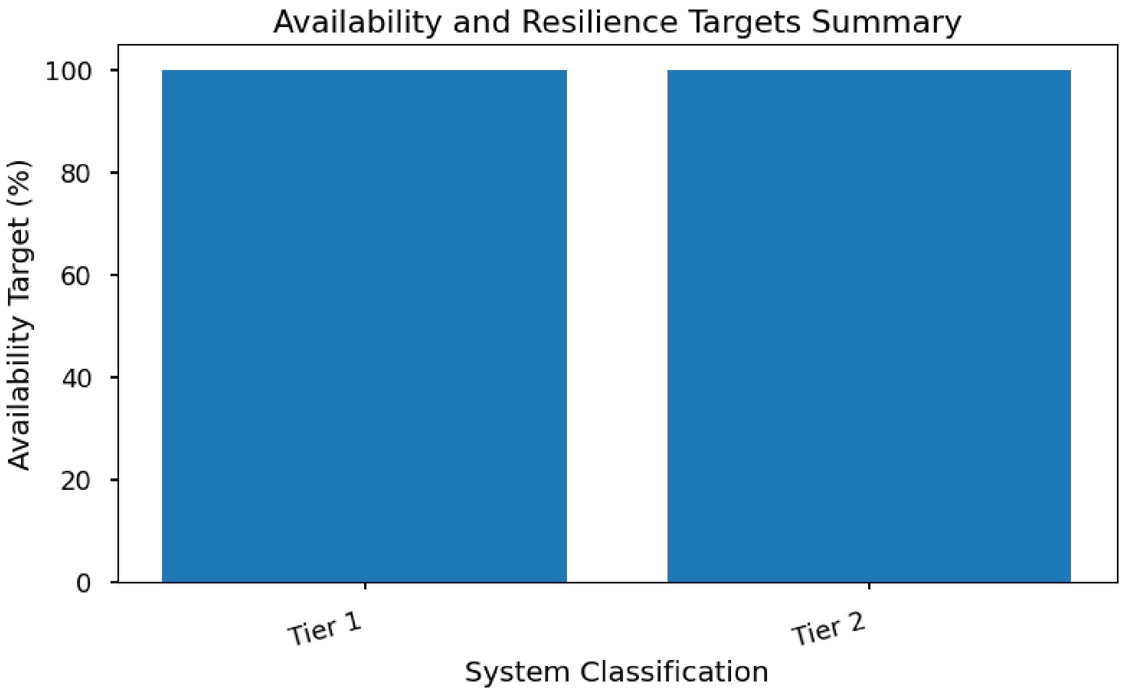
The following table delineates the architecture's availability tiers alongside p95 performance and scalability metrics for core enterprise services. These targets are established to ensure service continuity, minimize downtime, and maintain user experience for both Tier 1 (critical) and Tier 2 (important but non-critical) systems.

| **Classification** | **Availability Target** | **p95 Performance Target** | **Scalability Metric** |
|---|---|---|---|
| Tier 1 | ≥99.99% | ≤250ms response time | Horizontal scaling; auto-scaling groups |
| Tier 2 | ≥99.9% | ≤500ms response time | Manual scaling; scheduled capacity reviews |

## Resilience & RTO/RPO

Resilience principles and indicative Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets are established to guide architecture decisions and operational procedures. These targets are not detailed runbooks, but rather architectural guardrails.

- Design for fault tolerance at every layer (network, compute, storage).
- Automated failover for Tier 1 services; manual failover for Tier 2.
- Data replication across physically separated zones for critical assets.
- RTO (Tier 1): ≤2 hours.
- RTO (Tier 2): ≤8 hours.
- RPO (Tier 1): ≤15 minutes.
- RPO (Tier 2): ≤1 hour.
- Periodic resilience testing (chaos engineering, failover drills).
- Dependency minimization to reduce blast radius.
- Segmented recovery domains to isolate failures.



## Security-by-Design Controls (Across All Equipment Classes)

Security-by-design is foundational to Vmobile’s enterprise architecture and is systematically enforced across all IT equipment classes, infrastructure layers, and environments. Controls are implemented to ensure confidentiality, integrity, and availability of systems and data, with explicit mechanisms for device trust, network segmentation, artifact assurance, and collaboration safeguards. These controls are designed to meet regulatory requirements, mitigate risk, and support zero-trust operational principles. The following sections detail the control expectations and architectural stance for device, network, artifact, and collaboration domains.

## Device & Network Controls

Security controls are enforced across all endpoints, network devices, and supporting infrastructure. The architectural stance is as follows:

- **Secure Boot**: All managed endpoints (laptops, desktops, conference room PCs, badge readers, and network CPE) must enforce secure boot, preventing unauthorized code execution at startup.
- **Full-Disk Encryption**: All storage-equipped devices (laptops, desktops, room PCs, badge readers) utilize full-disk encryption with enterprise-managed keys. Encryption status is exported to compliance signals for IAM.
- **Signed Images**: Firmware and OS images for all device classes must be cryptographically signed. Only validated images are permitted for deployment/upgrades.
- **Secrets Management**: Device secrets (machine credentials, API keys, certificates) are provisioned and rotated via centralized secrets management systems. No hardcoded secrets are permitted in device images or configuration.
- **Hardware Authenticators**: FIDO2 keys and biometric devices are integrated for privileged access and device trust validation.
- **Patch Currency**: Devices must report patch status; only compliant devices are permitted network access.
- **Endpoint Telemetry**: EDR agents and MDM platforms collect and forward health, compliance, and security signals to central observability stacks.

### Network Control Points Mapping

The following table defines the mapping of network control points to identity/segment domains and microsegmentation strategies.

| Control Point | Identity/Segment Scope | Microsegmentation Strategy | Enforcement Mechanism | Example Equipment Classes |
|---|---|---|---|---|
| NGFW (Next-Gen Firewall) | User/Corp/Restricted | Identity-aware L4/L7 segmentation | Dynamic policy via IAM signals | SD-WAN edge, campus core, DC border |
| VLAN/VRF | Corp/Guest/Management | Per-device VLAN, | Port-based, | Wi-Fi APs, |

| | | | | |
|---|---|---|---|---|
| Segmentation | | VRF isolation | MAC-based assignment | switches, conference A/V |
| East-West Firewalls | Restricted/Management | Microsegmentation at workload level | Tag-based dynamic rules | DC compute, storage, badge readers |
| ACLs on CPE | Branch/User/Corp | Source/dest IP, identity mapping | Device compliance gating | Branch routers, badge readers |
| Wi-Fi SSID Segregation | Guest/Corp/Restricted | SSID-based policy, device posture | MDM/EDR compliance enforcement | Wi-Fi APs, mobile phones, laptops |
| Out-of-Band Management | Management Segment | Dedicated mgmt network, isolated | Credentialed access, logging | DC management switches, room PCs |

## Artifact & Collaboration Controls

To secure the software supply chain and collaboration platforms, the following controls are mandated:

- **SBOM/Dependency Scanning**: All deployed software (including endpoint agents, conference room systems, and network firmware) must include a Software Bill of Materials (SBOM). Automated scanning for vulnerabilities in dependencies is enforced prior to production deployment.
- **Artifact Signing**: All binaries, firmware, and configuration artifacts are signed with enterprise-controlled keys. Unsigned or tampered artifacts are rejected by deployment systems.
- **Data Loss Prevention (DLP) & Egress Controls**: DLP policies are applied at endpoints, collaboration platforms, and egress gateways. Sensitive data exfiltration is blocked or alerted on, with real-time enforcement at the network perimeter and collaboration suite.
- **Collaboration Guardrails**: Enterprise collaboration platforms (Teams, SharePoint, etc.) are configured to restrict sharing of sensitive content outside of the organization. Automated guardrails enforce classification, prevent unauthorized sharing, and log all policy violations for review.

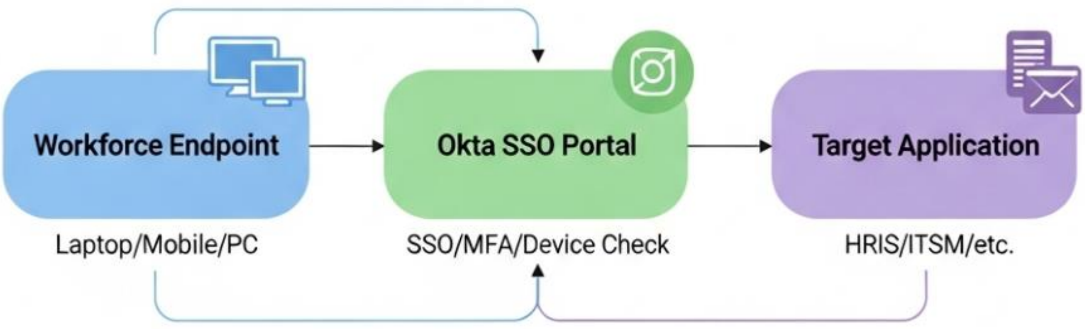
These controls collectively ensure that all IT equipment classes—ranging from endpoints and conference room systems to badge readers and network CPE—operate within a secure, compliant, and resilient architecture. Continuous monitoring and automated enforcement underpin the security posture across Vmobile's infrastructure.

## Reference Diagrams (ASCII/Text)

### Overview of Reference Diagrams for Key Architectural Flows

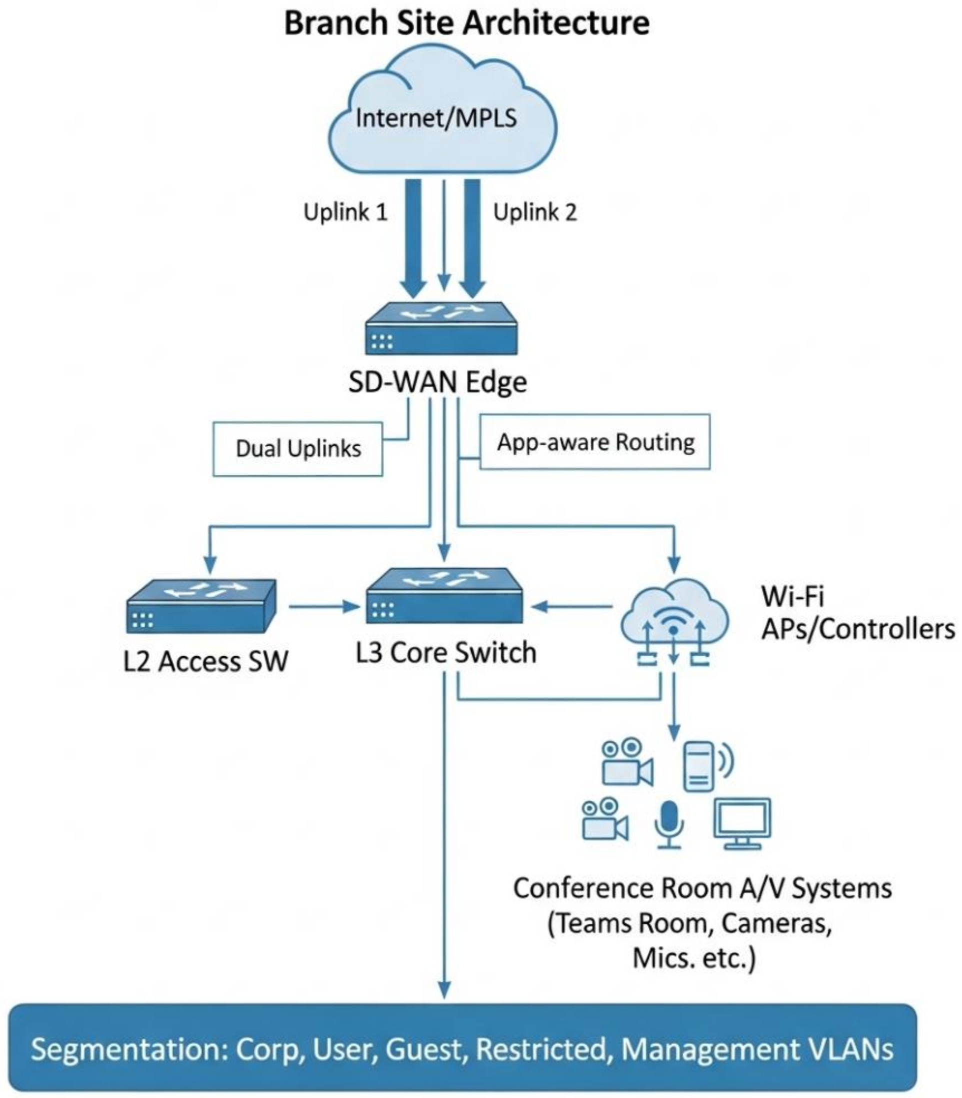
This section presents reference ASCII/text diagrams to visually illustrate critical architectural flows and topologies within the Vmobile enterprise environment. These diagrams are intended for technical stakeholders and architects, providing an unambiguous view of major integration points, control planes, and media paths. The diagrams cover workforce identity flows, branch site network layouts, data center logical topology, and conference room A/V media and management paths. These visuals serve as reference models for solution design, implementation, and ongoing architecture reviews.

#### Workforce SSO Flow (Okta + Device Posture)



- Device posture is validated via MDM/EDR signals before SSO is granted.
- Okta enforces MFA and checks for hardware authenticators (e.g., FIDO2 keys).
- Application access is contingent on both identity and endpoint compliance.

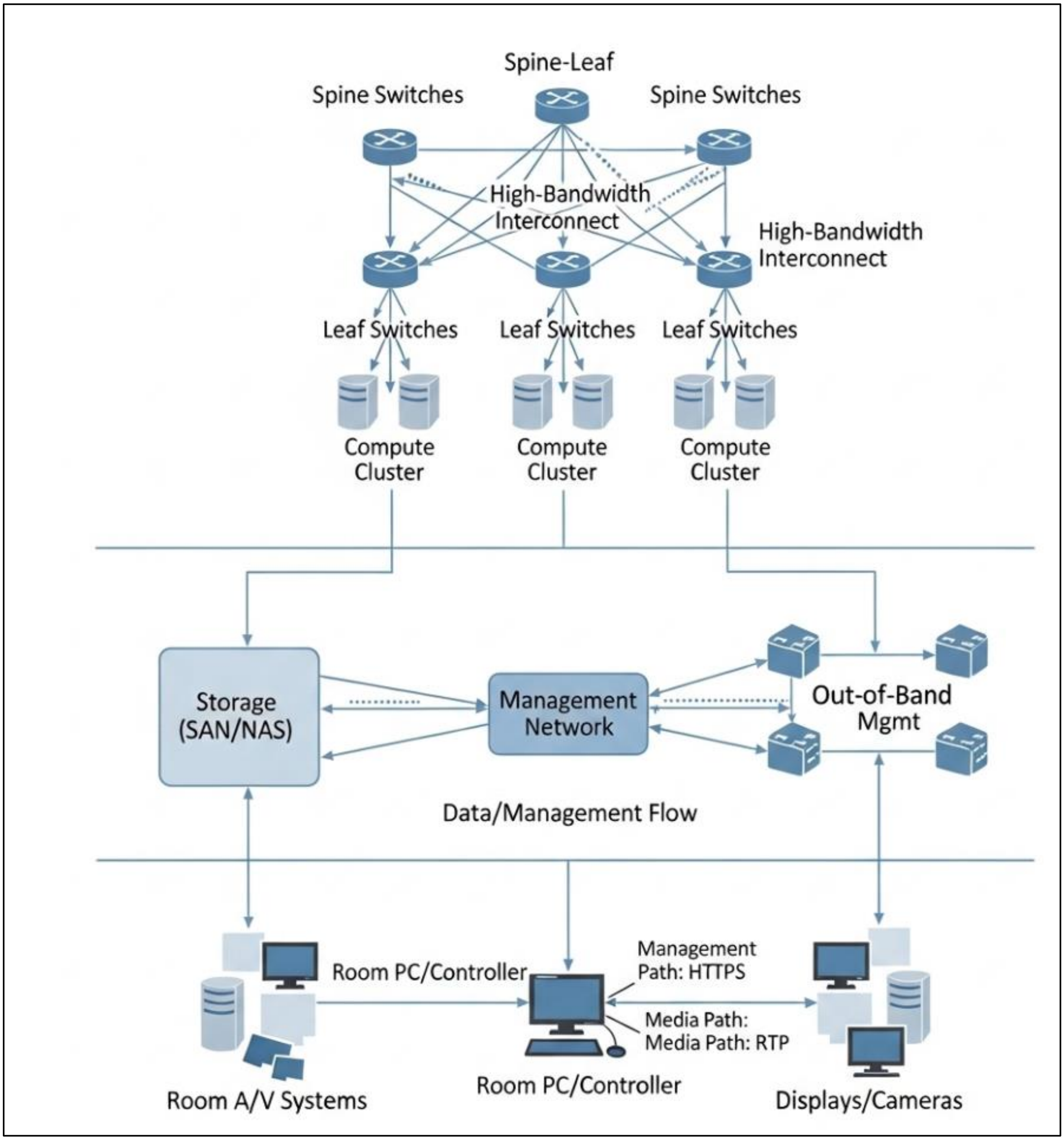
#### Branch Site: SD-WAN Edge → Core → Wi-Fi APs/Controllers → Conference A/V



**Topology Notes:**

- SD-WAN edge provides site connectivity with dual uplinks for resilience.
- LAN core switch manages segmentation and routing between access layers.
- Wi-Fi APs/controllers enforce SSID boundaries (corporate, guest).
- Conference Room A/V systems are segmented and monitored via management VLAN.

### DC Logical: Compute Clusters, Storage (SAN/NAS), Management Network, Out-of-Band Path



Legend:

- Spine/Leaf: DC network fabric for east-west, north-south traffic
- Storage: SAN/NAS for application and data platform
- Management Network: Segmented for admin/control traffic
- Out-of-Band: Isolated path for emergency access

- Room A/V: Media path (audio/video RTP), management path (HTTPS/TLS)

**Topology Notes:**

- DC backbone is spine/leaf for scalable, resilient connectivity.
- Storage and compute clusters are interconnected with management and OOB paths.
- Room A/V systems have distinct media (real-time audio/video) and management (control/config) channels.

## Interface Contracts & Port/Protocol Matrix (Selected)

### Introduction

This section defines the principal interface contracts and port/protocol mappings that underpin Vmobile's enterprise architecture. The intent is to provide a consolidated reference for integration points and communication pathways between critical systems, devices, and platforms. These mappings enable secure, observable, and reliable interoperability across Identity, Endpoint, Network, Collaboration, and Data domains. All interface contracts are governed by enterprise security and compliance policies; port/protocol selections are based on current best practices for confidentiality, integrity, and availability.

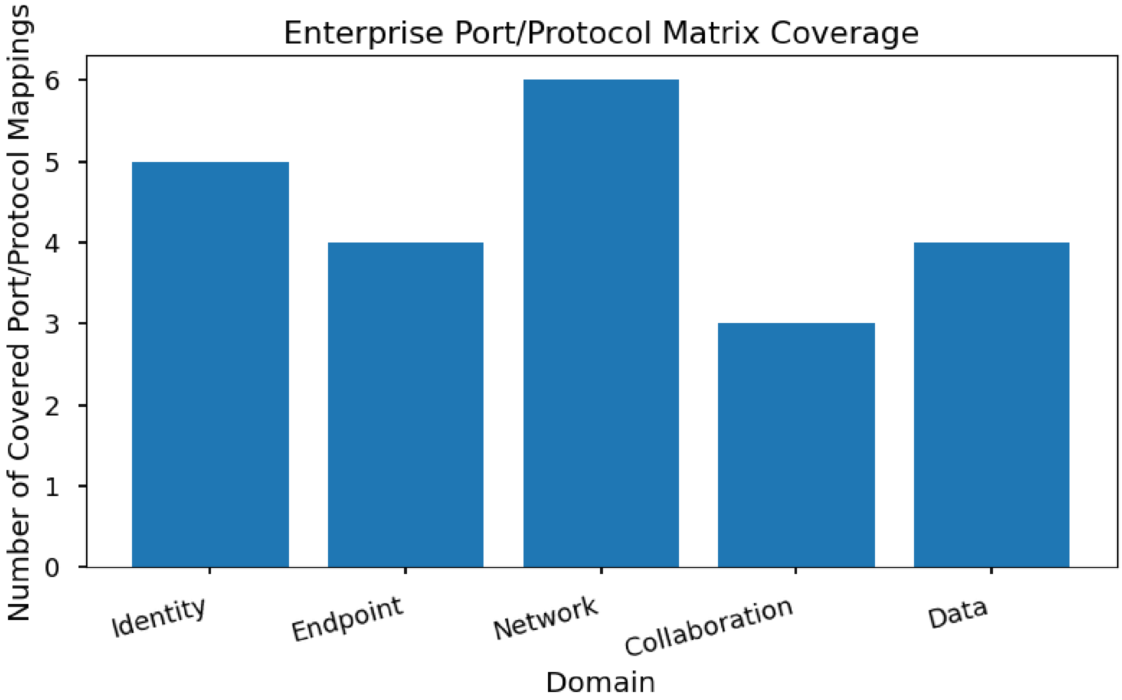
The matrix below enumerates the key flows and interfaces relevant for architectural planning, risk assessment, and operational oversight. End-user configuration details, deep vendor-specific port ranges, and troubleshooting guides are explicitly excluded per the blueprint scope. Reference to external guides (e.g., VPN setup, IAM training) is provided where necessary.

### Interface Contracts & Port/Protocol Matrix

| Domain | Interface/Flow | Protocol(s) | Port(s) | Directionality | Notes/Contract Highlights |
|---|---|---|---|---|---|
| Identity | SSO (OIDC/SAML via Okta) | HTTPS, SAML, OIDC | 443 | Bi-directional | AuthN/AuthZ; SSO trust; device posture included; SCIM for lifecycle provisioning. |
| Identity | SCIM Provisioning | HTTPS (REST) | 443 | Outbound to Okta | HRIS↔IAM user lifecycle (JML); attribute sync; API versioning and error handling per OpenAPI spec. |
| Device Compliance | Compliance Signal Export | HTTPS (REST) | 443 | Endpoint→IAM | Encryption, patch, EDR, firewall, screen |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | lock; device attestation; contract: JSON payload, signed requests. |
| Network Management | SSH for Device Admin | SSH | 22 | Admin→Device | Privileged access; JIT elevation; logged and monitored; key-based auth only. |
| Network Management | TLS for Mgmt APIs | HTTPS (REST/gRPC) | 443 | Bi-directional | SD-WAN, Wi-Fi controllers, NGFW; RBAC enforced; integration with SIEM for audit. |
| Network Telemetry | Syslog over TLS | Syslog (RFC 5425) | 6514 | Device→SIEM | Structured logs; identity anomaly detection; retention per data governance policy. |
| Network Telemetry | SNMP (if enabled) | SNMPv3 | 161/162 | SIEM/NMS↔Device | Used selectively for legacy gear; encrypted/authenticated; traps for health/availability. |
| Collaboration/Media | Web Conferencing (Teams/Zoom) | HTTPS, TURN/ICE | 443, 3478 | Bi-directional | Media relays; policy-level port ranges; no vendor-specific configs; identity-based access. |
| Collaboration/Media | Room A/V Control | HTTPS (REST) | 443 | Controller→Room PC | API contracts for device status, scheduling, firmware; managed via enterprise MDM. |
| Collaboration/Media | Media Streams | RTP/SRTP | 50000-59999 | Bi-directional | Audio/video; encrypted; flows segmented by room and user policy. |
| Printing | IPPS/IPP | HTTPS, IPP | 443, 631 | Endpoint→Printer | Secure print; RBAC enforced; job metadata logged for compliance. |
| Endpoint Management | MDM/EDR Agent Comm | HTTPS (REST) | 443 | Endpoint→Mgmt | Enrollment, policy updates, telemetry; admin-on-demand elevation; JSON contracts. |

| | | | | | |
|---|---|---|---|---|---|
| Data Platform | Data Lake/Warehouse Access | TLS (e.g., PostgreSQL) | 5432, 3306 | App→Data Platform | Row/column-level security; sensitivity labels; audit trails; contract: SQL over TLS, or REST for ELT. |
| Data Platform | ELT Streaming | HTTPS, Kafka, AMQP | 443, 9092 | Source→Lake | Batch/stream ingest; schema registry enforced; error/backoff contracts; HRIS/CRM/ERP connectors. |



- All flows are subject to segmentation and microsegmentation controls as defined in Section 5 (Network Architecture).
- Device compliance API exports are integrated with SIEM/SOAR workflows per Section 9 (Observability & Telemetry).
- Service ports for data platforms are selected examples; full inventory is maintained in the IT Hardware Inventory List (referenced, not included).
- Legacy protocols (e.g., SNMP) are used only where modern alternatives are not feasible and must be encrypted/authenticated.
- Collaboration/media ports are policy-level references; vendor-specific deep configurations are out of scope for this blueprint.

## Environments, CI/CD & IaC

Enterprise-grade IT and HRIS service delivery at Vmobile is underpinned by robust environment management, automated CI/CD pipelines, and rigorous Infrastructure-as-Code (IaC) controls. This blueprint establishes the foundational architecture for non-production and production environments, codified deployment gates, and secure automation practices. All environment promotion, change approvals, and infrastructure provisioning must adhere to standards outlined herein, with explicit separation of duties and auditability at every stage.

### Promotion Gates & Deployment Patterns

The environment lifecycle for all critical platforms (HRIS, ITSM, data, network automation, endpoint management) follows a strict promotion path, ensuring code quality, functional validation, and security posture at each gate. Deployment patterns are selected based on business impact and risk mitigation:

- Development (Dev)
- Testing (Test)
- Staging (Staging)
- Production (Prod)

Deployment strategies for user-facing and backend services include:

- Blue/Green Deployments
- Canary Releases
- Feature Flagging (where applicable)

These patterns facilitate controlled rollouts, rapid rollback on anomaly detection, and minimize user disruption. All promotions require automated and manual approval checkpoints, with change records tied to release artifacts.

### IaC Baselines & Secrets Management

Infrastructure provisioning for networks, security groups, and device management policies is entirely managed via IaC templates (e.g., Terraform, Ansible, CloudFormation). Architectural standards mandate:

- Declarative IaC for baseline network topologies, segmentation, and control planes.
- Source-controlled device policy definitions, including compliance signals and telemetry hooks.
- Automated PR-based change approvals, with mandatory peer review and security validation.

Secrets management is centralized in enterprise-grade vault solutions. All deployment credentials are:

- Short-lived (ephemeral) and scoped to the minimum necessary privilege.
- Rotated automatically per deployment cycle.
- Never embedded in code or IaC artifacts; referenced via secure vault integrations.

This approach ensures that all infrastructure changes are auditable, reproducible, and resilient against unauthorized access or configuration drift.

## Compliance Mapping (Guidance)

### Guidance on Compliance Mapping to SOC 2 / ISO 27001 and Privacy Alignment

This section provides authoritative guidance for mapping the Vmobile enterprise architecture blueprint to key compliance frameworks, specifically SOC 2 and ISO 27001. The controls and architectural stances described throughout this blueprint are designed to align with the requirements of these frameworks, with explicit hooks for identity management, change control, and data governance.

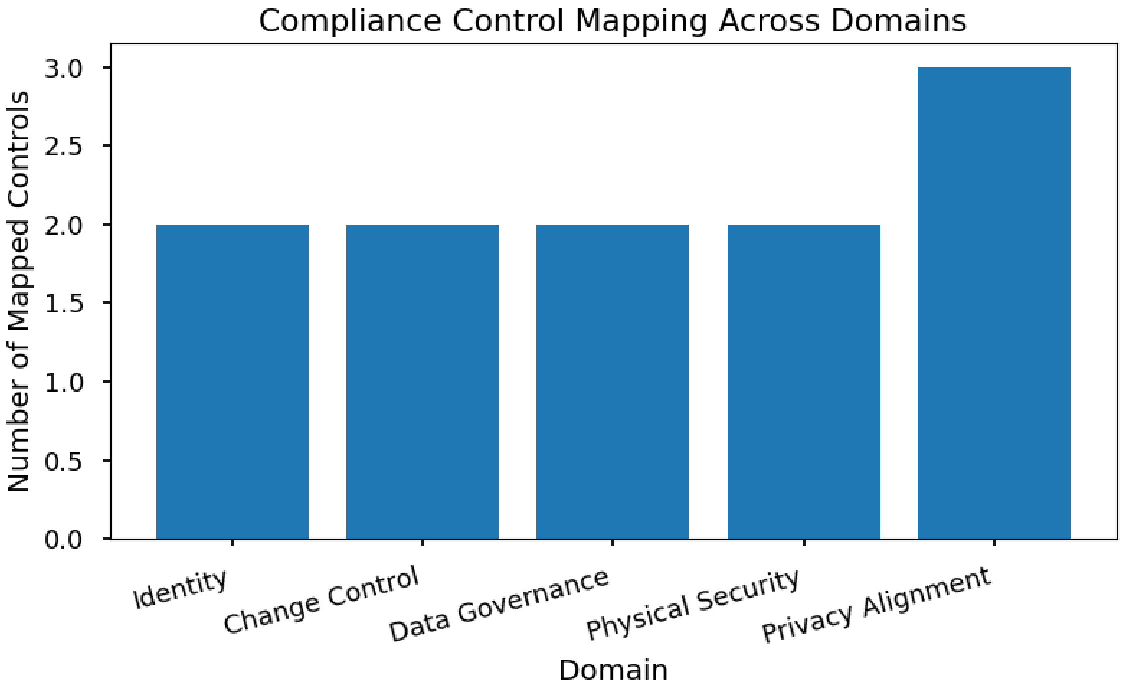
The compliance mapping herein is intended for use by Enterprise Architecture, IT Operations, Security, Networking, HRIS, and Facilities teams as a reference for control assurance and audit readiness. It does **not** include reporting outputs, incident/DR procedures, or end-user privacy workflow guidance; refer to the Non-Overlap list for those deliverables.

The privacy alignment pointers below are provided to support regulatory compliance (e.g., GDPR, CCPA) and internal privacy policies, focusing on classification, data subject rights (DSR) workflows, and physical security integration for DC and office environments.

### Control Hooks by Domain

| Domain | SOC 2 Control Hook | ISO 27001 Control Reference | Architectural Implementation Example |
|---|---|---|---|
| Identity | Access Controls, User Provisioning | A.9 Access Control, A.7 HR Security | SSO/MFA, JML lifecycle, quarterly recertification |
| Change | Change Management, Approval Flows | A.12 Operations Security, A.14 System Acquisition | CI/CD gates, PR-based approvals, IaC change logs |
| Data | Data Security, Retention, DLP | A.8 Asset Management, A.18 | Data retention tags, encryption, DLP |

| | | | |
|---|---|---|---|
| | | Compliance | controls |



## Privacy Alignment Pointers

- Data classification must be applied at ingestion and catalog layers, with sensitivity labels enforced via policy.
- Data Subject Rights (DSR) workflow integration for HRIS and CRM platforms, enabling timely response to access/erasure requests.
- Row/column-level security and legal hold mechanisms mapped to retention and privacy requirements.
- Privacy impact assessments (PIA) performed on new integrations and data flows.
- Physical security touchpoints:
  - Badge reader integration for DC/office access control.
  - CCTV coverage mapped to sensitive zones and entry/exit points.
  - Biometric device usage for restricted area authentication.

## Physical Security Touchpoints

- DC/office badge reader systems integrated with identity management platforms for real-time access logging.
- CCTV systems linked to facilities management and security overlays for incident review and monitoring.

- Biometric access devices (fingerprint, facial recognition) deployed at high-security locations, with authentication logs exported to SIEM.

## Technology Roadmap & Lifecycle Management

Vmobile's enterprise architecture mandates a proactive approach to technology adoption, lifecycle management, and refresh strategies across all IT and HRIS domains. This section defines the roadmap for introducing, maintaining, and retiring technology assets, ensuring alignment with business requirements, compliance standards, and operational excellence. The roadmap is architected to support continuous modernization, minimize technical debt, and uphold service levels across endpoint devices, network infrastructure, conferencing systems, and data platforms. Lifecycle management spans from initial selection and pilot evaluation, through production deployment, maintenance, and eventual decommissioning—guided by security-by-design principles, compliance mandates, and operational telemetry.

Lifecycle management is governed by centralized policy frameworks, leveraging automated asset tracking and compliance signal integration. Technology refresh cycles are planned based on vendor support timelines, security patching requirements, performance benchmarks, and evolving enterprise needs. All refresh decisions are subject to architectural review, with cross-functional input from IT Operations, Security, HRIS, and Facilities stakeholders.

### Roadmap Milestones

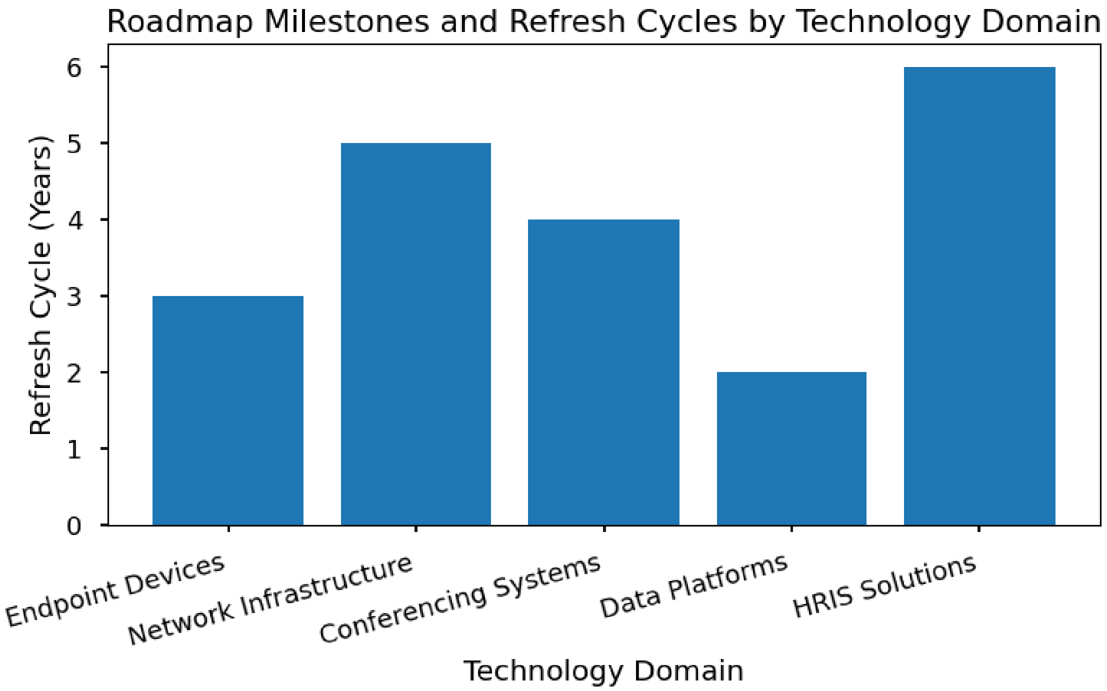
The following major milestones and refresh cycles are defined for Vmobile's key technology domains. Each milestone is mapped to business objectives, compliance requirements, and operational dependencies:

- **Endpoint Device Refresh (Laptops, Desktops, Monitors, Mobile Phones, SIMs):**
  - Standard refresh every 36 months for primary compute devices; 2 months for mobile handsets/SIMs aligned to carrier contracts.
  - Annual compliance review for device encrypiton, patch currency, and EDR signal integration.
  - BYOD revalidation and security posture assessment at onboarding and annually.
- **Conference Room A/V Systems:**
  - Full hardware refresh every 48 months, with interim firmware and software updates every 6 months.
  - Scheduled upgrades for Teams Room systems, cameras, microphones, and room scheduling panels, in line with collaboration platform releases.
- **Network Infrastructure (SD-WAN, Campus LAN/WLAN, Branch CPE):**

  - SD-WAN edge device lifecycle: 48-month replacement cycle, with interim OS upgrades every 12 months.
  - Wi-Fi APs/controllers: 36-month hardware refresh, quarterly security patching.
  - NGFW and VPN concentrators: 60-month replacement cycle, biannual policy review.
- **Data Center & Cloud Interconnect:**
  - Compute/storage clusters: 60-month refresh cycle, annual capacity and performance assessment.
  - Spine/leaf network upgrades every 48 months, with quarterly firmware patching.
- **Badge Readers/Biometric Devices:**
  - Hardware refresh every 60 months; quarterly firmware/security review.
  - Integration upgrades aligned with physical security system enhancements.
- **Data Platform (Lake/Warehouse):**
  - Staged technology adoption: pilot (Year 2), production rollout (Year 2–3), periodic upgrades (Year 4+).
  - Catalog and security label refresh every 12 months.
- **Application Integration & Middleware:**
  - API contract versioning and schema registry upgrades every 18 months.
  - Enterprise bus/ESB technology refresh every 48 months.
- **Observability & Telemetry Systems (SIEM/SOAR):**
  - SIEM platform refresh every 48 months; SOAR orchestration upgrades every 36 months.
  - Log/trace agent updates quarterly.

| **Equipment Class** | **Pilot/Adoption** | **Production Rollout** | **Maintenance/Upgrade** | **Refresh/Replacement** | **Decommissioning** |
|---|---|---|---|---|---|
| Laptops/Desktops | Year 1 | Year 2 | Quarterly | Year 3 | Year 4 |
| Mobile Phones/SIMs | Year 1 | Year 1 | Quarterly | Year 2 | Year 3 |
| Monitors/Printers | Year 1 | Year 2 | Annually | Year 3 | Year 4 |
| Conference Room A/V | Year 1 | Year 2 | Semi-annual | Year 4 | Year 5 |
| SD-WAN Edge Devices | Year 1 | Year 2 | Annually | Year 4 | Year 5 |
| Wi-Fi APs/Controllers | Year 1 | Year 2 | Quarterly | Year 3 | Year 4 |

| | | | | | |
|---|---|---|---|---|---|
| NGFW/VPN Concentrators | Year 1 | Year 2 | Biannual | Year 5 | Year 6 |
| DC Compute/Storage | Year 1 | Year 2 | Annually | Year 5 | Year 6 |
| Badge/Biometric Devices | Year 1 | Year 2 | Quarterly | Year 5 | Year 6 |
| Data Platform | Year 1 | Year 2 | Annually | Year 4 | Year 5 |
| API/Middleware | Year 1 | Year 2 | 18 months | Year 4 | Year 5 |
| SIEM/SOAR | Year 1 | Year 2 | Quarterly | Year 4 | Year 5 |



This timeline chart visualizes the lifecycle phases for each equipment class, from pilot and production rollout through maintenance, refresh, and decommissioning. All phases are subject to architectural governance, compliance review, and operational telemetry validation. Refresh cycles are planned to ensure optimal security posture, performance, and alignment with Vmobile's enterprise architecture standards.

## Integration with Third-Party Services

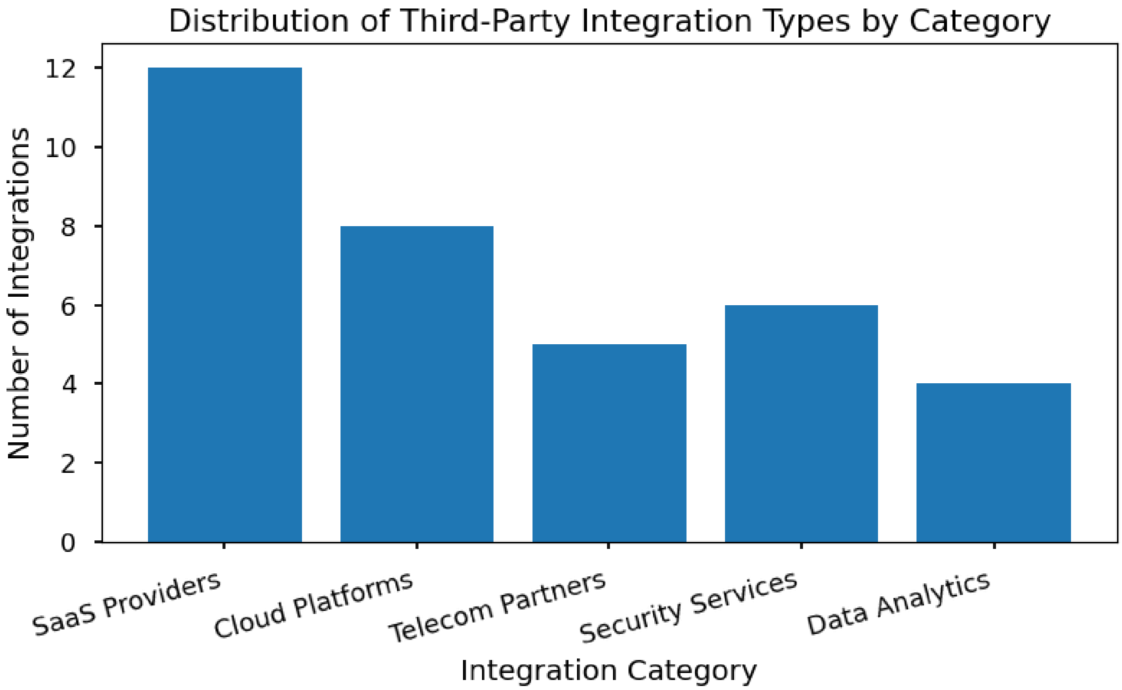
Integration with third-party services is a foundational aspect of Vmobile's enterprise architecture. The architectural stance prioritizes secure, scalable, and observable connections to external SaaS providers, cloud platforms, and telecom partners. All integrations are governed by zero-trust principles, API-first contracts, and explicit segmentation within the network and identity domains. Interfaces to third-party services are established via standardized protocols and encrypted transport layers, with all access subject to least privilege and continuous compliance monitoring. Data exchanged with external platforms is subject to data minimization, retention, and lineage controls as defined in Section 6 (Data Platform).

Integration endpoints are registered within the enterprise catalog and subjected to regular security reviews, including SBOM analysis and dependency scanning. All third-party connections are monitored for telemetry and anomaly detection, with SIEM/SOAR hooks enabled for rapid containment in the event of identity or data anomalies. Privileged access to third-party management consoles or APIs is managed via JIT elevation and quarterly recertification. Secrets and credentials required for integration are stored and rotated in enterprise-grade vaults, with short-lived tokens preferred over static keys.

### Third-Party Service Inventory

| Service Name | Category | Integration Type | Interface Protocols | Security Overlay | Data Scope | Segmentation Zone | Observability/ Telemetry |
|---|---|---|---|---|---|---|---|
| Microsoft 365 | SaaS Productivity | SSO, API | SAML, OIDC, REST | MFA, Conditional Access | Workforce Identity | Corp User Zone | SIEM, Audit Logs |
| Okta Identity Cloud | IAM | Directory Sync, SSO | SCIM, OIDC, SAML | MFA, JIT Privilege | Identity Metadata | Restricted/Privileged | SIEM, Access Logs |
| Salesforce | CRM | API, SSO | REST, OIDC | RBAC, IP Allowlisting | Customer Data | Corp User Zone | Metrics, API Tracing |
| Workday | HRIS | API, SSO | REST, SAML | Least Privilege, MFA | HR Data | Restricted Zone | SIEM, HRIS Logs |
| AWS Cloud | IaaS/PaaS | VPC Peering, API | HTTPS, IPSec, IAM | SGs, Secrets Vault | Compute/ Storage | DC/Cloud Interconnect | CloudWatch, SIEM |
| Cisco Webex | Conferencing | API, SSO | REST, OIDC | SSO, Network Segmentation | Media/Presence | Guest/Corp Segments | Room Telemetry |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Zoom Rooms | Conferencing | API, SSO | REST, OIDC | SSO, Network Segmentation | Media/Presence | Guest/Corp Segments | Room Telemetry |
| ServiceNow | ITSM | API, SSO | REST, OIDC | RBAC, Audit Logging | ITSM Data | Corp/Restricted Zone | SIEM, ITSM Logs |
| Twilio | Telecom API | API | HTTPS, REST | API Key Rotation, IP Whitelist | Messaging/Voice | Corp User Zone | API Metrics |
| Google Workspace | SaaS Productivity | SSO, API | SAML, OIDC, REST | MFA, Conditional Access | Workforce Identity | Corp User Zone | SIEM, Audit Logs |
| SAP SuccessFactors | HRIS | API, SSO | REST, SAML | RBAC, MFA | HR Data | Restricted Zone | SIEM, HRIS Logs |
| Oracle Cloud | IaaS/PaaS | API, VPC Peering | HTTPS, IPSec, IAM | SGs, Secrets Vault | Compute/Storage | DC/Cloud Interconnect | SIEM, Cloud Logs |
| AT&T VPN Gateway | Telecom Infra | IPSec, API | IPSec, REST | NGFW, VPN Auth | Network Traffic | Perimeter/Egress | VPN Logs, Metrics |



### Integration Risk Mitigation Strategies

- Enforce least privilege and RBAC on all third-party service accounts.
- Require MFA and conditional access for all external SaaS and cloud logins.
- Segment network traffic to/from third-party endpoints using NGFW and microsegmentation.
- Store and rotate all external service secrets in the enterprise vault; prefer short-lived tokens.
- Monitor all integration points with SIEM/SOAR for anomaly detection and automated containment.
- Regularly review SBOMs and scan for vulnerabilities in third-party connectors.
- Apply encryption for all data in transit to/from external services.
- Audit and recertify privileged access to third-party management consoles quarterly.
- Maintain an interface contract registry for all external APIs, with versioning and error models.
- Validate compliance alignment (SOC 2, ISO 27001) for all critical SaaS/cloud partners.

## Physical Infrastructure & Facilities Architecture

The physical infrastructure of Vmobile's enterprise environment forms the foundational layer upon which all IT, HRIS, and network architectures are deployed. This blueprint section outlines the architectural stance for physical elements—cabling, racks, power delivery, and environmental controls—ensuring that all systems operate with maximum reliability, scalability, and security. Physical infrastructure is treated as a critical control plane, directly influencing uptime, compliance, and the ability to support advanced IT and telecom workloads.

All cabling (fiber, copper, structured wiring) is specified to meet minimum Cat6A standards for data and PoE requirements, supporting high-density deployments and future expansion. Racks are standardized for 42U form factor, with enforced separation between network, compute, and storage domains. Power distribution units (PDUs) are dual-fed for redundancy; all critical equipment is backed by UPS and generator failover. Environmental controls—HVAC, fire suppression, and leak detection—are integrated with facilities monitoring systems and are subject to periodic audit.

Physical security overlays are embedded at every layer: badge readers and biometric devices at access points, CCTV coverage for all critical zones, and room scheduling panels for controlled access to conference facilities. All integration points are mapped to architectural domains to ensure consistent governance and telemetry.

### Facilities Integration Points

- **Badge Readers**
  - Integrated with identity management systems for real-time access control.
  - Physical access events exported to SIEM for anomaly detection.
  - Dual-authentication (badge + biometric) required for data center ingress.
- **Biometric Devices**
  - Used at high-security entrances (data center cages, executive areas).
  - Enrolled via HRIS workflows; tied to workforce identity sources.
  - Biometric events logged for compliance and audit.
- **Room Scheduling Panels**
  - Linked to calendaring and facilities management platforms.
  - Enforce access windows and occupancy limits for conference rooms.
  - Provide telemetry to facilities for utilization analytics.
- **Environmental Sensors**
  - Integrated with building management systems (BMS).
  - Feed real-time data on temperature, humidity, and air quality to observability platforms.
- **Power & Redundancy Systems**
  - PDUs, UPS, and generator status exported to network management and facilities dashboards.
  - Alarms and failover events logged for resilience reporting.

- **CCTV & Surveillance**
  - Video feeds integrated with physical security platforms.
  - Retention and access governed by privacy and compliance policies.

### Physical Infrastructure Component Mapping

| Physical Component | Architectural Domain | Primary Integration Points |
|---|---|---|
| Structured Cabling | Network | SD-WAN, Campus LAN/WLAN, Data Center Core |
| Racks | Compute/Storage/Network | DC Logical, Endpoint Segmentation |
| PDUs/UPS/Generators | Resilience/Availability | Network, Data Platform, Application Hosting |
| HVAC/Environmental | Observability | Telemetry Streams, Facilities SIEM |
| Badge Readers | Identity & Access | IAM, Facilities, Security Overlay |
| Biometric Devices | Identity & Access | HRIS, IAM, Security Overlay |
| Room Scheduling Panels | Endpoint/Facilities | Application Integration, Observability |
| CCTV Cameras | Security Overlay | Physical Security, Compliance Mapping |

## Performance Monitoring & Capacity Planning

Performance monitoring and capacity planning are foundational practices within Vmobile's enterprise architecture, ensuring that all IT domains—including endpoints, networks, and data platforms—operate within defined service levels and are prepared to scale in line with organizational growth and evolving business requirements. The approach is proactive and data-driven: monitoring is continuous, with automated telemetry collection and alerting across critical infrastructure and service layers. Capacity planning is cyclical, leveraging historical and predictive analytics to inform infrastructure upgrades, architectural refactoring, and resource allocation. Feedback loops from monitoring directly inform architecture updates, ensuring that both operational and strategic objectives are met.

Performance and capacity oversight is governed centrally, with domain-specific dashboards, threshold-based alerting, and regular review cycles. Metrics are aggregated and correlated across systems to identify bottlenecks, forecast future needs, and support evidence-based decision-making. This process enables IT Operations, Network Engineering, Data Platform, and Enterprise Architecture teams to maintain optimal performance, preempt resource exhaustion, and align infrastructure investments with business priorities.

## Monitoring Metrics

Key metrics tracked across the core domains include:

- **Endpoints**
    - CPU utilization
    - Memory usage
    - Disk I/O rates
    - Device health signals (patch status, encryption state)
    - EDR (Endpoint Detection & Response) event counts
    - Compliance posture (encryption, firewall, screen lock)
- **Network**
    - WAN/LAN throughput
    - Latency (site-to-site, campus, cloud interconnect)
    - Packet loss rates
    - SD-WAN edge utilization
    - Wi-Fi AP/client density
    - NGFW (Next-Generation Firewall) rule hit counts
    - VPN session concurrency
- **Data Platforms**
    - Data ingest rates (streaming vs batch)
    - Query response times
    - Storage utilization (lake/warehouse tiers)
    - ETL pipeline success/failure counts
    - Catalog lookup latency
    - Data retention compliance signals

The chart below illustrates the cyclical process for capacity planning and its integration with architecture updates:

1. **Continuous Monitoring:** Automated collection of performance and utilization metrics across endpoints, network, and data platforms.

2. **Threshold Evaluation:** Metrics are compared against predefined thresholds and service level objectives (SLOs).

3. **Alerting & Analysis:** Exceedance triggers alerting and root cause analysis; historical trends are reviewed for forecasting.

4. **Capacity Forecasting:** Predictive analytics model future resource needs based on growth patterns, seasonal spikes, and new service rollouts.

5. **Architecture Review:** Findings are fed into architecture review boards for prioritization and solution design.

6. **Resource Allocation & Scaling:** Infrastructure upgrades, reallocation, or refactoring are executed to address forecasted needs.

7. **Feedback Loop:** Post-implementation metrics are monitored to validate improvements; cycle repeats.

This closed-loop process ensures that Vmobile’s IT infrastructure remains resilient, performant, and scalable, with capacity planning tightly coupled to enterprise architectural governance.

## Vendor Management & Interoperability

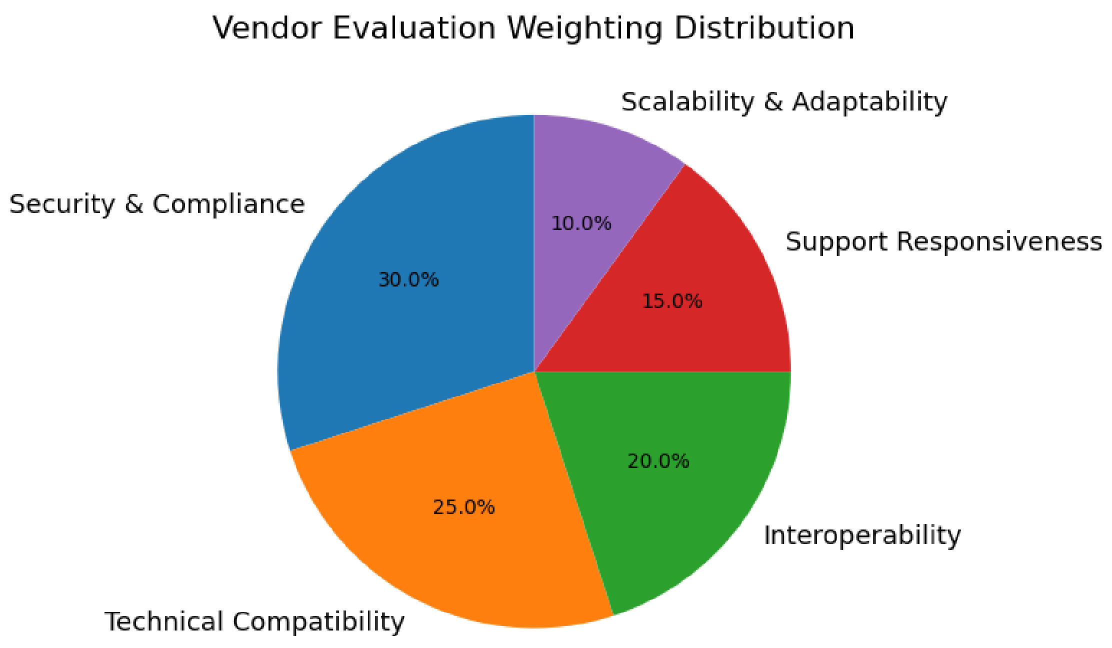
Effective vendor management and interoperability are foundational to Vmobile’s enterprise architecture strategy. The architectural stance mandates rigorous evaluation and ongoing oversight of all third-party technology providers, ensuring alignment with Vmobile’s principles of security-by-design, operational resilience, and seamless integration across the IT, HRIS, network, and facilities domains. Vendor selection and management processes are governed by standardized criteria that prioritize security, compliance, technical compatibility, and support responsiveness. Interoperability requirements are strictly enforced to maintain a unified, scalable, and adaptable enterprise environment, minimizing technical debt and vendor lock-in risks.

Vendors must demonstrate compatibility with Vmobile’s core architectural principles, including zero-trust, API-first integration, and observability-by-default. All solutions must support standardized protocols, enable robust management interfaces, and provide documented mechanisms for identity federation, telemetry export, and lifecycle integration. Ongoing vendor management includes periodic security assessments, compliance attestation, and proactive monitoring of interoperability with existing and future systems.

### Vendor Evaluation Criteria

| Evaluation Area | Criteria Description | Required Evidence/Artifacts | Weighting (%) | Notes/Examples |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Security | End-to-end encryption, secure boot, SBOM support, vulnerability disclosure process | Security whitepaper, SBOM, pen test results | 20 | Must support FIPS-validated crypto, signed images |
| Compliance | SOC 2, ISO 27001, GDPR, HIPAA, local regulatory alignment | Certificates, audit reports, privacy policies | 15 | Data residency and privacy controls required |
| Interoperability | Standards-based APIs (REST/OpenAPI, SCIM, SAML/OIDC), protocol support | API docs, interface contracts, protocol matrix | 25 | Must integrate with Okta, SIEM, MDM, etc. |
| Support & Maintenance | SLA terms, patch cadence, escalation procedures, EOL roadmap | SLA doc, support matrix, release notes | 10 | 24/7 support for Tier 1 platforms |
| Observability | Native support for structured logging, metrics, traces; SIEM/SOAR integration | Logging schema, SIEM integration guide | 10 | Syslog 6514, SNMP, REST event hooks |
| Identity Integration | SSO/MFA readiness, JML lifecycle hooks, privileged access controls | SSO config guide, SCIM endpoint, audit logs | 10 | Okta, FIDO2, JIT access required |
| Lifecycle Management | Automated provisioning/deprovisioning, device compliance signals, patching support | Lifecycle API docs, compliance schema | 5 | Must support HRIS/ITSM triggers |
| Physical Integration | Compatibility with site power/network standards, badge/CCTV integration | Hardware specs, cabling diagrams | 5 | For A/V, badge readers, network CPE |



## Interoperability Standards and Protocols

- RESTful APIs (OpenAPI v3.x)
- SAML 2.0 / OIDC for identity federation
- SCIM 2.0 for identity lifecycle
- Syslog (RFC 5424, port 6514 TLS) for logging
- SNMPv3 for network device telemetry
- HTTPS (TLS 1.2+) for all management interfaces
- IPPS/IPP for secure printing
- WebSocket (RFC 6455) for real-time eventing
- MQTT/AMQP for device telemetry (where applicable)
- LDAP(S) for directory integration
- FIDO2/WebAuthn for hardware authentication
- TURN/ICE for media relay in collaboration systems

These standards are mandatory for all new vendor integrations and are subject to periodic compliance review. Vendors unable to meet these interoperability requirements will not be approved for deployment within Vmobile’s enterprise environment.

## Future-State Architecture & Innovation

Vmobile's future-state enterprise architecture is engineered to enable secure, scalable, and resilient operations for a modern telecom workforce. This blueprint articulates a vision for a converged digital foundation, integrating HRIS, IT, network, and facilities domains under a unified architecture. The architecture is grounded in zero-trust, API-first, and observability-by-default principles, and is designed to anticipate the rapid evolution of business requirements, regulatory landscapes, and technology capabilities.

Key innovation areas include the strategic adoption of artificial intelligence and machine learning (AI/ML), advanced automation, edge computing, and next-generation observability. These initiatives will drive operational excellence, elevate user experience, and ensure compliance and governance at scale. The blueprint is intended to be adaptive, supporting continuous improvement and future integration of emerging technologies such as quantum-safe cryptography, intent-based networking, and autonomous endpoint management.

### Innovation Initiatives

- **AI/ML Integration**
  - Deploy machine learning models for predictive analytics in HRIS and ITSM workflows.
  - Utilize AI-driven security analytics for anomaly detection in identity, network, and endpoint telemetry.
  - Implement natural language processing (NLP) for automated HRIS case handling and IT ticket triage.
- **End-to-End Automation**
  - Automate joiner/mover/leaver (JML) lifecycle processes across identity and access domains.
  - Orchestrate network configuration and policy enforcement via programmable SD-WAN and cloud APIs.
  - Enable automated compliance checks and remediation for endpoint security and patch management.
- **Edge Computing Enablement**
  - Provision edge nodes at branch sites for low-latency processing of conference room A/V telemetry and local security events.
  - Deploy microservices at the edge for real-time data ingestion from badge readers and biometric devices.
  - Integrate edge analytics for rapid response to physical security incidents in facilities and data centers.
- **Advanced Observability**

  - Implement distributed tracing and telemetry for critical business flows (e.g., SSO, HRIS, ITSM).
  - Aggregate structured logs and metrics from all endpoint classes, network devices, and room systems.
  - Integrate SIEM/SOAR solutions for real-time detection and automated response to identity and network anomalies.
- **Emerging Technology Adoption**
  - Evaluate quantum-safe cryptography standards for future-proofing identity and data platforms.
  - Pilot intent-based networking for dynamic policy enforcement and segmentation.
  - Explore autonomous endpoint management leveraging AI for self-healing and compliance enforcement.

## Glossary

This section provides a consolidated glossary of telecom and IT terminology as referenced throughout this enterprise architecture.

### Key Terms and Definitions

- **API (Application Programming Interface)**

A standardized interface allowing applications or services to communicate and exchange data, typically over HTTP(S).

- **Asset**

Any hardware or software component managed within the enterprise IT environment, including endpoints, network devices, and room systems.

- **Batch ELT (Extract, Load, Transform)**

Data processing pattern where large volumes are processed in scheduled intervals, as opposed to real-time streaming.

- **Badge Reader**

Physical security device used for identity validation and access control at facility or data center entry points.

- **BYOD (Bring Your Own Device)**

Policy allowing workforce members to use personally-owned devices for corporate access, subject to segmentation and compliance controls.

- **Campus LAN/WLAN**

Local area network infrastructure supporting wired (LAN) and wireless (WLAN) connectivity within office/campus environments.

- **CI/CD (Continuous Integration/Continuous Deployment)**

Automated pipelines for building, testing, and deploying code and infrastructure changes.

- **Conference Room A/V Systems**

Integrated audio/video hardware in meeting spaces, including cameras, microphones, speakers, displays, and controllers.

- **Control Plane**

Logical layer managing configuration, policy enforcement, and orchestration of devices or services.

- **DC (Data Center)**

Centralized facility hosting compute, storage, and network resources for enterprise workloads.

- **Device Compliance Signal**

Telemetry exported from endpoints to indicate encryption, patch status, EDR presence, and other security attributes.

- **DLQ (Dead Letter Queue)**

Queue for storing messages or events that could not be processed successfully by downstream systems.

- **Domain Model**

Conceptual map of architecture domains: Identity, Network, Data, Applications, Endpoints, Observability, Security, Governance.

- **EDR (Endpoint Detection & Response)**

Security technology providing real-time monitoring and automated response on endpoint devices.

- **Endpoint**

User-facing device class (e.g., laptops, desktops, mobile phones, badge readers) managed by IT for access and compliance.

- **Event Bus**

Messaging infrastructure supporting asynchronous event delivery between applications or services.

- **FIDO2 Key**

Hardware-based authenticator supporting passwordless authentication flows and device trust.

- **Firewall (NGFW)**

Next-generation firewall providing application-aware traffic filtering and segmentation.

- **HRIS (Human Resources Information System)**

Centralized platform for workforce data, identity sources, and HR workflows.

- **IAM (Identity & Access Management)**

Systems and processes governing authentication, authorization, and access entitlements.

- **Idempotency**

API or integration property ensuring repeated requests produce the same effect.

- **JIT (Just-In-Time) Privileged Access**

Temporary elevation of access rights for specific tasks, with automated expiry.

- **JML (Joiner, Mover, Leaver)**

Workforce identity lifecycle events: onboarding, role changes, and offboarding.

- **Lakehouse**

Unified data platform combining features of data lakes and data warehouses, supporting structured and unstructured data.

- **Least Privilege**

Security principle enforcing minimum necessary access for users, devices, and services.

- **MDM (Mobile Device Management)**

Platform for provisioning, securing, and monitoring mobile endpoints.

- **Microsegmentation**

Fine-grained network segmentation restricting east-west traffic between workloads or devices.

- **Network CPE (Customer Premises Equipment)**

Edge networking hardware deployed at branch or campus sites.

- **Observability**

Capability to monitor, trace, and analyze system state via logs, metrics, and telemetry.

- **Okta**

Cloud-based identity platform supporting SSO, MFA, and workforce identity federation.

- **Out-of-Band Management**

Dedicated network path for device administration, isolated from production traffic.

- **Patch Currency**

Status indicating whether endpoint or infrastructure software is up-to-date with security patches.

- **Perimeter**

Network boundary where ingress/egress controls are enforced, typically via firewalls and VPN concentrators.

- **Port/Protocol Matrix**

Reference table mapping services to network ports and communication protocols.

- **RBAC (Role-Based Access Control)**

Access model assigning permissions based on user roles.

- **Recertification**

Periodic review and validation of access rights and privileges.

- **RED/USE Metrics**

Observability frameworks:

  - RED (Rate, Errors, Duration) for application monitoring
  - USE (Utilization, Saturation, Errors) for infrastructure monitoring

- **SD-WAN (Software-Defined WAN)**

Overlay network architecture enabling dynamic routing, segmentation, and dual uplink resiliency for branch sites.

- **Secrets Management**

Secure storage and rotation of credentials, keys, and tokens used by applications and devices.

- **Segment/Segmentation**

Logical separation of network or access domains (e.g., user, corporate, restricted, management, guest).

- **SIEM (Security Information & Event Management)**

Centralized platform aggregating security logs and performing anomaly detection.

- **SIM (Subscriber Identity Module)**

Secure hardware element in mobile phones for cellular authentication.

- **SOAR (Security Orchestration, Automation, and Response)**

Automated platform for incident response and remediation workflows.

- **Spine/Leaf Architecture**

Data center network topology providing scalable, high-bandwidth interconnects.

- **SSO (Single Sign-On)**

Authentication process enabling users to access multiple systems with a single credential.

- **Streaming ELT**

Real-time data ingestion and transformation pipeline.

- **Telemetry**

Automated reporting of device or service health, status, and events.

- **VPN (Virtual Private Network)**

Encrypted tunnel for remote access to corporate resources.

- **Wi-Fi SSID Segmentation**

Separation of wireless networks for corporate, guest, and restricted access.