

SASE + AI Integration Blueprint

Secure access, intelligent operations, and consistent policy across branches, remote users, cloud services, and data centers.



CONNECT

SD-WAN and resilient access

PROTECT

Identity and cloud security

IMPROVE

AI-assisted visibility and response

Enterprise architecture and implementation guide

October 2026

SASE + AI Architecture Guide

Seven-page architecture sequence: executive model, control planes, AI operations, rollout, security services, and measurable outcomes.

01

Executive architecture

Users, connectivity, SASE policy, applications, telemetry and governed AI.

3

02

Control + data planes

Identity context, policy orchestration, enforcement and application services.

4

03

AI operations workflow

Collect, normalize, correlate, analyze, recommend, approve and audit.

5

04

Implementation roadmap

Discover, assess, design, pilot, deploy and operate.

6

05

SASE security services

ZTNA, SWG, CASB, FWaaS, DLP and DNS security.

7

06

Enterprise outcomes

Security, experience, operations, resilience, governance and cost visibility.

8

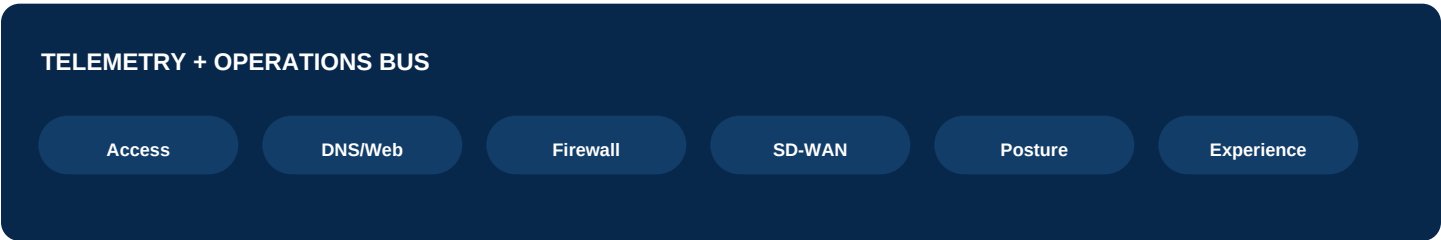
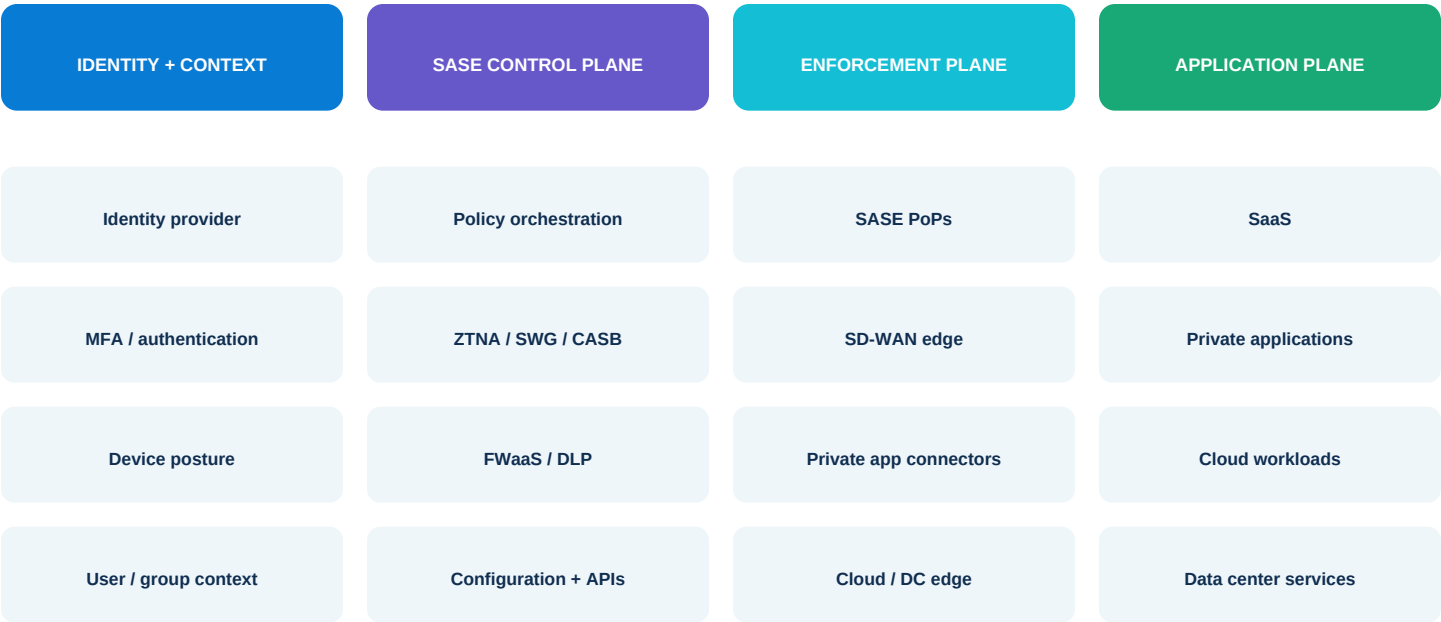
SASE + AI Reference Architecture

A layered enterprise model connecting users and sites to applications through policy-driven access, security, telemetry, and governed AI.



Reference Architecture - Control & Data Planes

Separate identity context, policy intent, enforcement, applications, telemetry, and operations for clearer governance and troubleshooting.



AI-ASSISTED OPERATIONS

Correlate events, highlight anomalies, summarize incidents, and recommend actions. Production-impacting changes require named human approval.

GOVERNANCE GUARDRAILS

Least privilege | evidence and confidence | sensitive-data controls | output validation | change approval | audit logging | tested rollback.

AI Operations - Signal to Governed Action

Use AI to accelerate investigation and decision support while retaining explicit human control over consequential production actions.

01

COLLECT

Identity, endpoint, DNS, web, firewall, ZTNA, CASB and SD-WAN telemetry.

02

NORMALIZE

Align time, user/device identifiers, policy IDs, severity and application context.

03

CORRELATE

Group related identity, network, security and application events.

04

ANALYZE

Surface anomalies, experience degradation and likely contributing factors.

05

RECOMMEND

Draft investigation, containment, routing or policy options with evidence.

06

APPROVE + AUDIT

Named operator validates evidence, approves action, and preserves rollback history.

GUARDRAILS

Human approval | evidence before action | least privilege | audit trail | sensitive-data controls | tested rollback

Implementation Roadmap - Architecture to Operations

Deploy in controlled waves: establish the baseline, validate the architecture, pilot policies, then scale with measurable governance.

1 DISCOVER

Inventory users, sites, applications, circuits, identities, controls and dependencies.

2 ASSESS

Baseline access, latency, loss, incidents, trust boundaries, gaps and experience.

3 DESIGN

Define SASE components, resilience, telemetry, AI governance and success measures.

4 PILOT

Test a bounded cohort, normal access, denied access, failover, exceptions and rollback.

5 DEPLOY

Expand by migration wave with change control, training, runbooks and verification.

6 OPERATE

Tune policy and analytics, measure outcomes, review exceptions and forecast capacity.

DECISION GATES

Architecture approved -> pilot criteria met -> rollback verified -> operational handoff accepted -> KPI review active

SASE Security Services Architecture

Cloud-delivered security services apply consistent identity, web, application, firewall, and data controls across users and locations.

1

ZTNA

Private application access based on identity, device posture, and least privilege.

2

SWG

Secure web access, malware protection, URL/category controls, and inspection.

3

CASB

SaaS discovery, application governance, session controls, and data-aware policy.

4

FWaaS

Cloud-delivered network access control and inspection for Internet-bound traffic.

5

DLP

Data classification and policy enforcement tuned to business workflows.

6

DNS SECURITY

Block malicious domains and add early protection before connections are established.

UNIFIED POLICY PRINCIPLE

Coordinate identity, network, application and data controls through shared policy, telemetry, change governance and operations.

Enterprise Outcomes & Measurement

Translate the SASE + AI architecture into measurable security, experience, operations, resilience, governance, and cost outcomes.

SECURITY

Track policy coverage, unauthorized attempts, incident quality, and alert precision.

EXPERIENCE

Measure access success, p95 latency, packet loss, application response, and complaints.

OPERATIONS

Monitor MTTD/MTTR, exception age, recommendation acceptance, and rollback rate.

RESILIENCE

Test failover success, service-point reachability, path diversity, and recovery time.

GOVERNANCE

Review coverage by user/site/app, approvals, audit completeness, and overdue reviews.

COST VISIBILITY

Assess circuit utilization, service overlap, support effort, and capacity trends.

EXECUTIVE REVIEW CADENCE

Baseline -> pilot review -> deployment-wave review -> monthly service review -> quarterly architecture review.

Identity, Zero Trust & Secure Access

Make identity, device posture, application context, and least privilege the foundation of access decisions.

IDENTITY ASSURANCE

Integrate identity provider, MFA, groups, roles, and joiner/mover/leaver lifecycle.

DEVICE POSTURE

Use device health and management state to permit, restrict, or deny access.

APPLICATION ACCESS

Grant users access to named applications rather than broad network segments.

CONTEXT-AWARE POLICY

Evaluate user, device, application, location, risk, and session context.

EXCEPTIONS

Record owner, justification, compensating control, approval, and expiry.

AUDITABILITY

Retain authentication, policy decision, access, and administrative change evidence.

ZERO TRUST PRINCIPLE

Verify explicitly | use least privilege | assume breach | continuously evaluate context and session risk.

SD-WAN & Connectivity Architecture

Engineer resilient, application-aware connectivity that works with cloud-delivered SASE policy and inspection.

PATH DIVERSITY

Document primary and backup access for critical branches, campuses, and data centers.

APP STEERING

Set path policy for real-time, business-critical, SaaS, and bulk traffic.

CLOUD ON-RAMPS

Optimize paths to SASE service points, SaaS platforms, and public cloud environments.

FAILURE TESTING

Exercise circuit, edge, provider, and service-point failure scenarios.

CAPACITY

Maintain headroom for peak traffic and credible failure-state operation.

VISIBILITY

Correlate path, latency, loss, jitter, utilization, and application experience.

INTELTEL CONNECTIVITY FIT

Coordinate SD-WAN with Internet, IP VPN, Cloud Connect, and enterprise routing where appropriate.

Security Service Edge - Policy Stack

Coordinate cloud-delivered security controls as one policy and operations framework.

ZTNA

Identity- and device-aware access to private applications with least privilege.

SWG

Web access control, malware protection, category policy, and inspection.

CASB

SaaS discovery, application governance, session controls, and data-aware policy.

FWaaS

Cloud-delivered network policy and inspection for Internet-bound traffic.

DLP

Classify sensitive data and tune controls to business workflows before strict blocking.

DNS SECURITY

Block known malicious destinations early and add visibility to domain activity.

SHARED POLICY MODEL

Identity + device + application + data + network context -> policy decision -> enforcement -> telemetry.

Private Application Access Architecture

Move from broad network reachability to controlled, application-level access for private services.

DISCOVER APPS

Catalog applications, owners, hostnames, protocols, dependencies, and user populations.

PLACE CONNECTORS

Deploy private-access connectors close to applications with appropriate resilience.

DEFINE POLICY

Map identity groups and device posture to specific application access.

MIGRATE

Pilot low-risk applications before complex, legacy, or high-dependency services.

VERIFY

Test authorized workflows, denied access, connector failure, and rollback.

DECOMMISSION

Retire legacy remote-access paths only after dependency and recovery validation.

ACCESS DESIGN GOAL

Users connect to authorized applications without receiving unnecessary network-level access.

Telemetry & Data Architecture

Create trusted, normalized operational signals for SASE observability and AI-assisted analysis.

SIGNAL SOURCES

Identity, endpoint, DNS, SWG, CASB, FWaaS, ZTNA, SD-WAN, and application telemetry.

NORMALIZATION

Align time, user/device IDs, policy IDs, application identifiers, severity, and location.

DATA QUALITY

Monitor missing feeds, late events, schema changes, duplicates, and clock drift.

RETENTION

Define retention periods based on operations, investigation, compliance, and cost needs.

DATA PROTECTION

Apply masking, regional storage, encryption, and role-based query access.

INTEGRATION

Feed SIEM, ITSM, observability, reporting, and approved AI-analysis workflows.

ARCHITECTURE RULE

AI quality depends on telemetry quality: incomplete or inconsistent signals must be visible to operators.

AI Anomaly Detection Architecture

Use evidence-backed analytics to prioritize meaningful deviations without treating every anomaly as an incident.

BEHAVIOR SIGNALS

Review unusual access, denials, locations, transfer patterns, and session behavior.

NETWORK SIGNALS

Detect abnormal latency, loss, path changes, utilization, and application degradation.

CONTEXT

Combine asset criticality, identity, device, application, and recent change context.

VALIDATION

Analysts distinguish expected change, faults, misconfiguration, and potential compromise.

MODEL TUNING

Track precision, false positives, alert volume, drift, and group-level performance.

ESCALATION

Tie severity and response to evidence strength, impact, confidence, and business criticality.

AI OPERATING PRINCIPLE

Anomaly detection surfaces evidence for review; it does not independently authorize high-impact action.

AI-Assisted Incident Response

Accelerate investigation, containment planning, and communications while preserving human approval.

CORRELATE

Group related identity, network, security, and application events into an incident view.

SUMMARIZE

Draft concise timelines, affected users/apps, indicators, and likely contributing factors.

RECOMMEND

Suggest verification, containment, policy, or routing options with expected impact.

APPROVE

Require named operator approval for blocking, isolation, or production policy changes.

EXECUTE

Use controlled workflows with least privilege, change tracking, and rollback.

LEARN

Review outcome, false positives, missed signals, and playbook improvements.

AUDIT REQUIREMENT

Preserve evidence -> recommendation -> approver -> action -> outcome -> rollback history.

Digital Experience Architecture

Measure the user journey across identity, network, SASE service points, and applications.

DNS

Track lookup success, response time, resolver path, and security policy effects.

AUTHENTICATION

Measure sign-in success, MFA friction, identity latency, and device posture checks.

CONNECTIVITY

Observe path, latency, loss, jitter, tunnel health, and service-point reachability.

APPLICATION

Measure connection success, transaction response, availability, and dependency health.

CORRELATION

Connect user complaints to device, path, security policy, and application context.

OPTIMIZATION

Prioritize changes based on recurring evidence and measurable user impact.

EXPERIENCE GOAL

Security controls and network changes should be evaluated against both risk reduction and user experience.

Architecture Options & Selection

Choose a SASE operating model based on coverage, integration, resilience, governance, and exit risk.

SINGLE PROVIDER

Potentially simpler integration; validate feature depth, regions, resilience, and lock-in.

MULTI-PROVIDER

Specialist capability may improve fit; plan for integration and operational complexity.

HYBRID MIGRATION

Integrate existing controls while defining a target state and retirement sequence.

REGIONAL DESIGN

Evaluate service-point presence, data handling, support, and regulatory requirements.

PORTABILITY

Document APIs, policy export, logs, dependencies, and provider-exit considerations.

SCORECARD

Score security, latency, resilience, logging, APIs, governance, operations, and cost.

DECISION PRINCIPLE

Select architecture against documented requirements and test evidence, not feature lists alone.

Risk & Control Architecture

Design controls for provider, policy, identity, AI, data, and operational failure scenarios.

PROVIDER OUTAGE

Use diverse access, tested failover, and documented alternate service behavior.

POLICY ERROR

Stage changes, peer review, test scope, monitor impact, and maintain rapid rollback.

IDENTITY FAILURE

Plan resilient authentication and controlled emergency-access procedures.

AI ERROR

Treat generated findings as advisory until validated against source evidence.

DATA EXPOSURE

Minimize telemetry, restrict access, protect sensitive fields, and govern retention.

CHANGE RISK

Use ownership, approvals, maintenance windows, validation, and post-change review.

CONTROL OBJECTIVE

Every material failure mode should have an owner, detection method, response path, and tested recovery action.

Pilot Reference Architecture

Prove access, security, performance, resilience, AI workflows, and operational readiness before enterprise scale.

PILOT COHORT

Choose representative branches, remote users, devices, SaaS, and private applications.

BASELINE

Capture current access success, latency, incidents, complaints, and operational effort.

TEST CASES

Normal access, denied access, lost device, link failure, service failure, and false positives.

SUCCESS CRITERIA

Define measurable targets and acceptable variance before testing begins.

ROLLBACK

Document and test reversal of routing, access, security, and application changes.

GO / NO-GO

Review evidence with business, security, network, identity, cloud, and operations owners.

PILOT OUTPUT

Validated architecture + exception list + runbooks + KPI baseline + approved deployment-wave plan.

Deployment & Transition Architecture

Scale through controlled migration waves with verification, training, documentation, and operational handoff.

WAVE DESIGN

Group sites and users by dependency, risk, geography, support capacity, and change window.

PARALLEL OBSERVATION

Compare old and new paths before enabling high-impact enforcement.

CHANGE CONTROL

Use approved templates, maintenance windows, validation checks, and rollback criteria.

TRAINING

Prepare service desk, network, security, identity, cloud, and application support teams.

HANDOFF

Deliver topology, policy inventory, dashboards, runbooks, contacts, and escalation paths.

WAVE REVIEW

Capture defects, exceptions, user impact, and improvements before the next migration wave.

TRANSITION GOAL

Each wave should leave the environment more standardized, observable, supportable, and recoverable.

SASE + AI Operating Model

Use a governed lifecycle from discovery through optimization, with clear ownership across technical domains.

DISCOVER + ASSESS

Validate environment, business outcomes, dependencies, risks, baseline metrics, and constraints.

DESIGN + GOVERN

Agree architecture, ownership, service levels, standards, policy, data, and AI guardrails.

DEPLOY + TRANSITION

Pilot, migrate, verify, document, train, and formally hand over operations.

OPERATE

Monitor security, access, experience, capacity, incidents, exceptions, and provider performance.

OPTIMIZE

Tune policy, routing, analytics, service placement, automation, and operational workflows.

REVIEW

Provide executive service reviews, recommendations, capacity forecasts, and technology roadmaps.

INTELTEL LIFECYCLE

Discover -> Assess -> Design -> Govern -> Deploy -> Transition -> Operate -> Optimize.

Measurement & Governance Framework

Use a shared scorecard to connect security posture, user experience, operations, resilience, and governance.

SECURITY KPIs

Policy coverage, incidents, unauthorized attempts, alert precision, and containment quality.

EXPERIENCE KPIs

Access success, p95 latency, loss, application response, and user-impact trends.

OPERATIONS KPIs

MTTD/MTTR, ticket volume, exception age, rollback rate, and automation acceptance.

RESILIENCE KPIs

Failover success, service reachability, recovery time, and failure-state capacity.

GOVERNANCE KPIs

Coverage, approvals, audit completeness, policy review age, and ownership gaps.

EXECUTIVE VIEW

Summarize business impact, major risks, service trends, investment priorities, and roadmap.

REVIEW CADENCE

Operational dashboards continuously | service review monthly | architecture and governance review quarterly.

SASE + AI Next Steps

Turn the reference architecture into a practical readiness assessment, pilot, and governed enterprise rollout.

1. ALIGN OUTCOMES

Agree priority applications, user groups, security outcomes, experience targets, and business constraints.

2. ASSESS CURRENT STATE

Inventory identity, WAN, remote access, security controls, cloud, applications, telemetry, and operations.

3. DESIGN TARGET STATE

Define architecture, resilience, policy model, service placement, telemetry, AI guardrails, and ownership.

4. PILOT + VALIDATE

Test a bounded cohort against documented access, security, experience, failover, and rollback criteria.

5. SCALE

Deploy in controlled waves with runbooks, training, service reviews, and measurable governance.

6. OPTIMIZE

Use telemetry and AI-assisted analysis to refine policy, capacity, experience, and operations.

START YOUR INTELTEL SASE + AI READINESS ASSESSMENT

Build a prioritized architecture roadmap aligned with security, connectivity, cloud, operations, and business goals.