Service Brief

Migration

majentai

Cisco Secure Access (CSA) Migration

The Cisco Secure Access (CSA) Migration is a structured engagement designed to move customers from legacy VPN, proxy, DNS security, or alternate SSE/SASE platforms into Cisco Secure Access with controlled risk and clear operational readiness. Majentai guides discovery, policy mapping, and phased cutover so teams can modernize access without unnecessary disruption.

Overview

This CSA Migration is a focused engagement designed to deliver a validated transition from a legacy access environment into Cisco Secure Access with limited operational risk, with a clear path to broader production adoption. This aligns SIA, SPA, and RAVPN capabilities, maps legacy controls into the target architecture, and establishes the governance, validation, and cutover model to scale confidently.

- Legacy-to-CSA migration strategy
- SIA policy and DNS transition
- SPA app access migration
- Coexistence and phased cutover
- Operations handoff and governance

Business Outcomes

This engagement reduces disruption risk by moving legacy access controls into CSA through phased validation, coexistence planning, and controlled rollout. It gives stakeholders clearer operational visibility, confidence in policy outcomes, and a foundation for broader modernization across users, applications, and locations.

- Reduce user impact during migration
- Improve confidence in target-state controls
- Strengthen operational ownership after cutover
- Create a scalable Secure Access foundation

At a Glance

Objectives

- Translate current controls into a CSA-aligned target state
- Migrate SIA/SPA/RAVPN capabilities with controlled risk
- Deliver a phased path to production readiness

Scope

- Migration from one or more legacy access platforms
- SIA/SPA/RAVPN workstreams within agreed scope
- Pilot, coexistence, cutover, and operational transition support

Deliverables

- Migration design and rollout plan
- Policy mapping and validation evidence
- Runbook, closeout, and roadmap package

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders, confirms migration scope and success criteria, and assesses the current environment across legacy VPN, proxy, DNS, identity, endpoint, network, and application dependencies to define risks, coexistence needs, and cutover constraints.

Phase 2: Solution Design and Planning

Majentai defines the target CSA architecture, policy mapping approach, identity and RBAC model, Secure Client rollout plan, SPA connector strategy, validation criteria, and phased migration sequence required for a controlled transition.

Phase 3: Build, Implement and Validate

Majentai configures the CSA baseline, supports identity and policy implementation, enables SIA, SPA, and RAVPN migration workstreams, executes pilot and cutover waves, and tunes approved exceptions for production readiness.

Phase 4: Operations & Recommendations

Majentai delivers runbooks, knowledge transfer, governance guidance, legacy decommission recommendations, and next-step priorities so customer teams can assume ownership and continue hardening and scaling the environment after migration.

Majentai is a world-class Cybersecurity services provider, dedicated to implement, integrate and operate the most resilient Cybersecurity platforms using proven state-of-the-art technologies. With a team of seasoned experts and cutting-edge technology, we deliver comprehensive solutions tailored to our clients' unique needs, ensuring their digital assets remain secure in an increasingly complex cyber landscape.

For more information or to engage our services, please contact us at info@majentai.com or visit https://majentai.com