Service Brief

Proof of Value

majentai

Cisco Secure Access (CSA) PoV

This Cisco Secure Access (CSA) PoV is a pilot-first engagement designed to validate Secure Internet Access (SIA) and Secure Private Access (SPA) outcomes in a greenfield environment. Majentai configures the platform, enables users and applications, validates results, and delivers the artifacts needed to transition toward production.

Overview

This Cisco Secure Access (CSA) PoV is a focused engagement designed to prove value quickly with controlled scope and limited risk, with a clear path to broader rollout after pilot validation. The PoV validates policy enforcement, private application access, identity targeting, and operational visibility while establishing the foundation required to implement and scale Secure Access with confidence.

- SIA policy validation and enforcement
- SPA application access enablement
- Identity and group mapping integration
- Pilot onboarding and test execution
- Operational handoff and recommendations

Business Outcomes

The Majentai CSA PoV reduces adoption risk by proving security controls, private access workflows, and operational readiness in a limited pilot before broader rollout begins, giving stakeholders early validation before they commit to a larger implementation. It gives stakeholders clearer evidence, tuning insight, and a more confident path into production planning.

- Prove value before full implementation
- Reduce disruption through controlled pilot scope
- Improve confidence in policy enforcement
- Prepare operations for production expansion

At a Glance

Objectives

- Validate measurable SIA and SPA pilot outcomes
- Confirm identity, policy, and access workflows work as designed
- Deliver a production-minded path beyond the PoV

Scope

- Greenfield PoV for SIA, SPA, and RAVPN pilot use cases
- Up to 10 internet access policies and 5 pilot applications
- Up to 2 client profiles, with limited connector, tunnel, or DLP scope as applicable

Deliverables

- PoV design and test plan
- Validation evidence and tuning log
- Closeout report and implementation roadmap

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders on pilot users, applications, success metrics, and test scenarios, then validate readiness across identity, endpoints, network dependencies, and the access requirements needed to support both SIA and SPA use cases.

Phase 2: Solution Design and Planning

Define the PoV architecture, identity integration, SIA policy baseline, Secure Client approach, connector placement, and application onboarding plan, then finalize execution sequencing, validation evidence requirements, and acceptance gates.

Phase 3: Build, Implement and Validate

Configure the CSA tenant, implement SSO and group targeting, build SIA and SPA policies, onboard pilot users and applications, execute testing, capture evidence, and tune policies or exceptions based on observed results.

Phase 4: Operations & Recommendations

Deliver the closeout report, operations runbook, knowledge transfer, and phased implementation recommendations needed to transition from pilot validation into production planning, broader rollout, and long-term operational ownership.

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