Service Brief

Assessment

majentai

Cisco Secure Access (CSA) Assessment

This Cisco Secure Access (CSA) Assessment is a readiness engagement designed to determine whether an organization is prepared to adopt Secure Internet Access (SIA) and Secure Private Access (SPA). Majentai validates technical and operational dependencies, identifies risks, and delivers a roadmap for pilot planning, remediation, and readiness at scale.

Overview

This CSA Assessment is a focused readiness engagement designed to clarify what it will take to deploy CSA with lower risk and better alignment, with a clear path to pilot execution and phased enforcement. The assessment validates identity, endpoint, network, application, and operational prerequisites while establishing the foundation required to implement and scale Secure Access with confidence.

- Identity and SSO readiness
- Endpoint onboarding feasibility
- Network and egress prerequisites
- Application and connector requirements
- Governance and support model

Business Outcomes

The CSA Assessment reduces rollout risk by validating prerequisites early, aligning stakeholders on scope and governance, and giving teams a prioritized path from readiness to controlled implementation. It also creates a clear set of actions that support pilot planning, stronger stakeholder alignment, and confident execution.

- Reduce surprises before implementation begins
- Improve pilot scoping and decision quality
- Strengthen governance and support readiness
- Accelerate time to secure adoption

At a Glance

Objectives

- Validate CSA readiness across core technical domains
- Identify gaps, risks, and deployment dependencies
- Define a practical pilot and rollout path

Scope

- SIA, SPA, RAVPN, or combined readiness assessment scope
- Current-state review across identity, endpoints, network, and operations
- Planning engagement only, with pilot use cases and limited in-scope apps

Deliverables

- Readiness findings by domain
- Pilot recommendation and implementation gates
- Prioritized remediation roadmap

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders, confirm whether the assessment covers SIA/SPA/RAVPN, define success criteria, and gather the current-state inputs required to assess identity, endpoint, network, and operational readiness.

Phase 2: Solution Design and Planning

Assess target-state requirements across IdP, endpoint deployment, DNS and egress design, connector placement, and application onboarding needs, then define the recommended pilot scope, constraints, and sequencing.

Phase 3: Build, Implement and Validate

Validate key readiness assumptions through targeted proof points, confirm prerequisite feasibility, and produce the dependency backlog, remediation priorities, and go or no-go criteria required before implementation begins.

Phase 4: Operations & Recommendations

Define the operating model, policy governance workflow, support expectations, and reporting needs, then deliver a phased roadmap that guides remediation, pilot execution, and broader CSA adoption.

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