

# Cisco Secure Access (CSA)

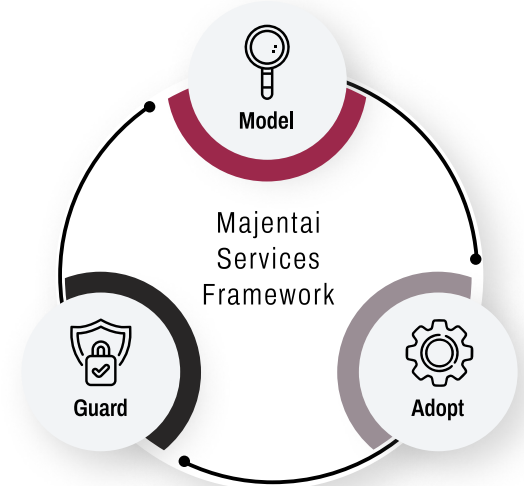
Cisco Secure Access (CSA) helps teams modernize user and application access with a cloud-delivered architecture that supports secure internet and private application access, plus policy-based control across distributed users, devices, and environments. Majentai supports the full CSA lifecycle with offerings spanning assessments, implementations, and day-2 operational support.

## Overview

Cisco Secure Access (CSA) delivers the most value when it is treated as a program, not a one-time deployment, and Majentai supports that lifecycle end-to-end. Through our Model, Adopt, Guard framework, we help teams move from early planning and pilot validation to phased rollout and sustainable operations, using practical sequencing and durable day-2 workflows so Secure Access stays effective as requirements evolve.

### Common outcomes

- Reduce risk tied to legacy VPN and fragmented remote access.
- Improve visibility into user access, policy behavior, and application exposure.
- Turn Secure Access into an operational capability, not just a deployment.
- Accelerate adoption with a phased, lower-risk rollout path.
- Improve policy consistency with clearer ownership and governance.



## Service Offerings

**Model:** Discovery, validation, and planning to align goals, requirements, and rollout.

- **CSA Workshop:** A structured working session to align stakeholders, validate current-state assumptions, and define architecture, governance, and rollout priorities for Secure Access.
- **CSA Assessment:** A focused readiness engagement to identify technical and operational prerequisites, clarify deployment risks, and deliver a practical roadmap for pilot planning and implementation.
- **CSA PoV:** A limited-scope proof-of-value engagement to validate Secure Internet Access and Secure Private Access outcomes, confirm success criteria, and produce clear next steps for broader rollout.

**Adopt:** Deploy the solution, validate outcomes, and prepare for production expansion.

- **CSA MVP:** A timeboxed deployment designed to prove early value with a controlled pilot scope, validated access workflows, and a defined path to scale into production.
- **CSA Implementation:** A greenfield deployment engagement to establish the CSA tenant, core identity and policy integrations, and a phased rollout model that supports production adoption.
- **CSA Migration:** A structured transition from legacy VPN, proxy, DNS security, or alternate SSE/SASE platforms into Cisco Secure Access, with coexistence planning, phased cutover, and stabilization support.

**Guard:** Day-2 support to keep Secure Access stable, supportable, and aligned.

- **CSA Guardian Support:** A post-deployment support engagement that provides governed incident response, policy tuning, operational validation, and structured workflows to sustain and improve CSA over time.

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](mailto:info@majentai.com) or visit <https://majentai.com>