Service Brief

Guardian Support

majentai

Cisco Secure Access (CSA) Guardian Support

Cisco Secure Access (CSA) Guardian Support is a structured post-deployment support engagement designed to keep Secure Access stable, secure, and operationally sustainable after implementation. Majentai provides governed incident response, policy tuning, visibility validation, and controlled change execution across SIA, SPA, RAVPN, identity, endpoints, and day-2 operations.

Overview

This Cisco Secure Access (CSA) Guardian Support is a managed support engagement designed to sustain Secure Access after deployment with structured workflows, governed changes, and repeatable operational practices. The service stabilizes user and application access while establishing the support foundation required to improve visibility, reduce disruption, and scale operations with confidence.

- Incident response and break/fix support
- Policy tuning and exception governance
- Identity and access workflow validation
- Operational dashboards and runbooks
- Knowledge transfer and health checks

Business Outcomes

The CSA Guardian Support service reduces operational risk by combining structured support, governed policy management, and validated visibility into one sustainable operating model. It gives stakeholders stronger confidence, clearer ownership, and a practical path to improve Secure Access maturity over time.

- Reduce access disruption across users and apps
- Improve confidence in policy governance decisions
- Strengthen operational visibility and readiness
- Accelerate steady-state CSA adoption and scale

At a Glance

Objectives

- Maintain stable and supportable CSA day-2 operations
- Reduce user and application access disruption
- Establish governed support and change workflows

Scope

- SIA-only, SPA-only, or combined CSA support
- Coverage across identity, endpoints, policies, and connectors
- Recurring touchpoints, health checks, and posture reviews

Deliverables

- Guardian Support operating model and workflows
- Runbook set and monitoring plan
- Ongoing operations roadmap and recommendations

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders, confirm support scope across SIA/SPA/RAVPN review the current CSA baseline, capture pain points and known issues, and define coverage expectations, KPIs, reporting cadence, and required operational inputs.

Phase 2: Solution Design and Planning

Define the steady-state support model, including incident handling, policy governance, exception management, monitoring expectations, change categories, escalation paths, and the recurring rhythm needed to support CSA consistently.

Phase 3: Build, Implement and Validate

Operationalize the model by executing incident triage, validating identity targeting, Secure Client behavior, and SPA connector health, tuning policies based on evidence, and validating dashboards, log workflows, and known-good test procedures.

Phase 4: Operations & Recommendations

Majentai transitions the service into steady-state operations through knowledge transfer, formalized review cadence, confirmed support ownership, and a prioritized roadmap for ongoing optimization, expansion, and long-term CSA maturity.

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