

Cisco Secure Workload (CSW) Guardian Support

Majentai CSW Guardian Support provides reactive, ticket-based operational support for your Cisco Secure Workload environment, with defined response targets during business hours and a monthly timebox for predictable delivery. This service helps keep policy enforcement healthy, resolve incidents quickly, and sustain day-2 operations as your CSW deployment grows.

Overview

CSW Guardian Support is a managed support engagement designed to keep your Cisco Secure Workload deployment stable and operational through structured intake, daily health verification, and expert issue resolution, with a clear path to optimize policies and expand coverage over time. The service provides a predictable monthly block of hours and defined business-hour response targets to support day-2 operations without adding internal headcount.

- Ticket-based reactive support (Jira intake)
- Daily CSW platform health checks
- MACD support for workloads and policy
- Incident troubleshooting and resolution
- Ongoing configuration documentation

Business Outcomes

CSW Guardian Support reduces operational risk and accelerates CSW value by ensuring day-2 support coverage, faster incident response, and consistent governance as your environment evolves.

- Reduced downtime and policy enforcement drift
- Faster operational changes through structured MACD
- Improved visibility into CSW platform health
- Stronger run-state documentation and governance

Engagement Phases

Phase 1: Strategy and Discovery

Align on covered assets, access requirements, ticketing intake (Jira), priorities, and success criteria, then confirm the current CSW deployment context and support workflow expectations.

Phase 2: Solution Design and Planning

Define health check coverage, escalation paths, change-control expectations, and reporting cadence, including which integrations/connectors are considered critical for monitoring.

Phase 3: Build, Implement and Validate

Execute daily health checks and respond to tickets for MACD and incident resolution, validating enforcement services, agent health, and platform integrity through controlled troubleshooting and change execution.

Phase 4: Operations & Recommendations

Run ongoing support within the monthly hour block, maintain documentation, facilitate quarterly service reviews, and provide recommendations for upgrades, optimization, and next-step expansion.

At a Glance

Objectives

- Maintain CSW operational health and enforcement continuity
- Respond to incidents with defined business-hour targets
- Support ongoing MACD and day-2 platform changes

Scope

- Up to 40 support hours per month (1-hour increments)
- Covered CSW deployment and defined covered assets
- Business hours: Mon–Fri, 7:00am–7:00pm CT

Deliverables

- Daily health check findings and issue identification
- Completed MACD and incident tickets with resolution notes
- Updated configuration documentation for changes

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>