Service Brief

MVP

majentai

Cisco Secure Workload (CSW) MVP

The Majentai CSW MVP establishes a reference architecture aligned to your hybrid environment, integrates the most relevant infrastructure and metadata sources, builds an accurate application dependency map for the pilot applications, and validates microsegmentation policies before moving to phased enforcement with rollback planning and operational readiness.

Overview

This Cisco Secure Workload (CSW) MVP is a pilot-first engagement designed to deliver fast, measurable outcomes with limited scope and controlled risk, with a clear path to expand into full production. The MVP validates core CSW capabilities quickly and safely, while establishing the governance and operational foundation required to run CSW as a repeatable program.

- Application dependency mapping and workload visibility
- Microsegmentation and Zero Trust segmentation policy
- Workload risk scoring and vulnerability context (where in scope)
- Policy simulation, enforcement, and continuous verification
- Integration into existing ITSM and cloud or virtual infrastructure (where in scope)

Business Outcomes

The CSW MVP reduces risk quickly by turning visibility into enforceable micro-segmentation for a focused pilot. Majentai establishes repeatable operations, validates policy impact safely, and delivers a clear path to expand across more applications, environments, and teams.

- Reduce lateral movement with least-privilege microsegmentation.
- Accelerate time-to-value with staged policy rollout.
- Establish repeatable operations: roles, workflows, knowledge transfer.
- Deliver roadmap to expand coverage across environments.

At a Glance

Objectives

- Establish CSW reference architecture for the pilot scope
- Deliver ADM-driven microsegmentation with safe, staged enforcement
- Enable repeatable operations (roles, workflows, knowledge transfer)

Scope

- Up to 2 business applications (prod or non-prod)
- Up to 2 native integrations (connectors or orchestrations)
- Up to 100 agents

Deliverables

- Segmentation strategy and use case matrix
- CSW high-level design and integration overview
- Closeout report with recommendations and next steps

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders, scope, and decision rights, define initial segmentation use cases and success criteria, and confirm the current-state telemetry, infrastructure, and metadata readiness required to support the pilot applications.

Phase 2: Solution Design and Planning

Define the MVP target design, select up to two integrations, establish labeling and grouping conventions, and finalize the onboarding plan for agents and any supplemental telemetry sources.

Phase 3: Build, Implement and Validate

Build application dependency maps, translate observed flows into segmentation policy, validate impact through simulation and monitoring, and progress into phased enforcement through the approved change process.

Phase 4: Operations & Recommendations

Finalize operational workflows and ownership, complete knowledge transfer, and stabilize CSW for day-to-day operations. Review MVP outcomes and prioritize next-step improvements and expansion across additional applications, integrations, and scope.

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