Service Brief

Proof of Value

majentai

Cisco Secure Workload (CSW) PoV

This Cisco Secure Workload (CSW) PoV is a pilot-first engagement designed to validate segmentation strategy, telemetry readiness, and enforcement workflows with focused scope and controlled risk. Majentai aligns the platform to the environment, integrates key data sources, builds visibility, and moves from policy design through simulation to operational transition.

Overview

This Cisco Secure Workload (CSW) PoV is a focused engagement designed to prove value quickly with limited scope and controlled risk, with a clear path to rollout. The PoV validates core CSW capabilities across visibility, telemetry, policy design, and enforcement readiness while establishing the governance and operational foundation required to support long-term segmentation outcomes.

- Application dependency mapping and workload visibility
- Microsegmentation and Zero Trust policy design
- Workload risk scoring and vulnerability context
- Policy simulation, enforcement, and verification
- Telemetry and metadata source integration

Business Outcomes

The CSW PoV reduces operational and segmentation risk by turning visibility into validated policy decisions before enforcement is applied. Majentai establishes a practical architecture, aligns stakeholders around governance and change control, and delivers a clear path to expand segmentation coverage across additional workloads, applications, and environments with stronger day-to-day operability.

- Reduce lateral movement with better segmentation control
- Improve confidence before policy enforcement decisions
- Accelerate rollout with phased validation approach
- Establish supportable operating model for expansion

At a Glance

Objectives

- Establish CSW reference architecture for the target environment
- Validate policy design with controlled simulation and approval workflows
- Enable repeatable operations, ownership, and knowledge transfer

Scope

- Up to 2 business applications in scope
- Production or non-production pilot application coverage
- Relevant compute, telemetry, and metadata integrations

Deliverables

- CSW high-level design and requirements artifacts
- Onboarding plan and application tracking outputs
- Policy design and closeout recommendations

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders, define use cases and decision rights, and assess current infrastructure, telemetry, tagging, and compliance context needed to support accurate visibility and pilot segmentation outcomes.

Phase 2: Solution Design and Planning

Define the target CSW architecture, integration points, segmentation model, and label design, then finalize onboarding methods, supplemental telemetry inputs, and rollout controls for the pilot.

Phase 3: Build, Implement and Validate

Build dependency maps, translate validated traffic flows into policy structure, simulate impact, and progress through controlled enforcement stages using approved workflows, monitoring, and rollback considerations.

Phase 4: Operations & Recommendations

Document operating responsibilities, support knowledge transfer, validate recommended enforcement approaches, and deliver next-step guidance to stabilize the platform and prepare for broader rollout.

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