Service Brief

Migration

majentai

Cisco Secure Workload (CSW) Migration

Majentai's Cisco Secure Workload (CSW) Migration service is a structured engagement designed to transition customers from an existing microsegmentation/uSeg platform to a greenfield CSW deployment, with a controlled path from discovery to policy enforcement. The engagement builds dependency maps, and enables operational governance for sustained segmentation.

Overview

This CSW Migration is a phased engagement designed to move customers from a legacy uSeg platform to Cisco Secure Workload with minimal operational risk, with a clear path to expand segmentation coverage over time. The service establishes target architecture, telemetry ingestion, and policy governance while delivering validated dependency mapping and a controlled simulate-to-enforce rollout.

- uSeg-to-CSW transition strategy
- Telemetry and metadata onboarding
- Application dependency mapping (ADM)
- Microsegmentation policy design
- Phased enforcement and operations handoff

Business Outcomes

The CSW Migration reduces segmentation risk and accelerates time-to-value by establishing a repeatable migration model from legacy controls into CSW, backed by validated telemetry and stakeholder alignment. Majentai delivers a phased path to enforcement, strengthens operational readiness, and a clear path to segmentation.

- Reduced enforcement risk through simulation-first rollout
- Improved visibility via validated telemetry and labels
- Faster policy authoring from ADM-driven evidence
- Clear ownership model, runbooks, and next-step roadmap

At a Glance

Objectives

- Define migration scope, governance, and segmentation success criteria
- Establish CSW architecture, integrations, and labeling strategy
- Build, validate, and enforce policies with controlled risk

Scope

- Migration from an existing uSeg platform to greenfield CSW
- Hybrid coverage (on-prem, cloud) as applicable
- Pilot scope based on agreed number of applications

Deliverables

- Segmentation strategy and requirements package
- CSW high-level design and onboarding plan
- Policy design artifacts and closeout recommendations

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders and decision rights, define segmentation use cases and compliance drivers, and assess uSeg configs, inventory, telemetry readiness, and tagging quality to identify migration gaps.

Phase 2: Solution Design and Planning

Define the target CSW architecture, integration points (virtualization, cloud, Kubernetes, CMDB/identity, ITSM/vulnerability tools), labeling conventions, and an onboarding plan that sequences environments and applications safely.

Phase 3: Build, Implement and Validate

Deploy CSW and onboard workloads/telemetry, build dependency maps, translate validated flows into policy intents, run simulation and impact analysis, and execute phased enforcement with change control and rollback.

Phase 4: Operations & Recommendations

Document operational workflows and role-based responsibilities, deliver knowledge transfer sessions, stabilize remaining enforcement, and provide closeout recommendations and a roadmap to expand coverage and integrations.

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