Service Brief

Implementation

majentai

Cisco Secure Workload (CSW) Implementation

Cisco Secure Workload (CSW) Implementation is a greenfield CSW engagement for dependency mapping, workload visibility, and Zero Trust microsegmentation. Majentai aligns stakeholders, integrates data sources, builds the dependency map, and moves policies from simulation to enforcement with operational handoff.

Overview

This engagement establishes CSW as a durable segmentation and visibility foundation across on-prem, private cloud, and public cloud workloads (VMs, bare metal, and containers/Kubernetes). It focuses on high-fidelity telemetry and metadata, a practical scope tree and labeling strategy, and a governance model that supports safe progression from simulate to monitor to enforce.

- Application dependency mapping (ADM) and workload inventory
- Segmentation policy design and simulation
- Controlled policy enforcement and verification
- Telemetry and metadata integrations
- Operational workflows and role-based handoff

Business Outcomes

The CSW Implementation reduces segmentation risk and accelerated time-to-control by establishing reliable workload context, validated dependency mapping, and a phased enforcement path. Majentai delivered workflows and artifacts that supported Day 2 operations and future expansion.

- Faster ADM to policy decisions
- Lower enforcement risk through simulation
- Consistent labels and scope structure
- Clear operating model for Day 2

At a Glance

Objectives

- Stand up CSW architecture aligned to hybrid strategy
- Establish trustworthy telemetry, labels, and dependency maps
- Progress segmentation policies to safe enforcement

Scope

- Greenfield CSW implementation as primary platform
- Integrations across compute, identity/tagging, and telemetry sources
- Target applications: prod and non-prod (customer-defined list)

Deliverables

- Segmentation strategy and use case matrix
- CSW high-level design (HLD) and scope tree
- Onboarding plan / segmentation policy design artifacts

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders and decision rights, define segmentation use cases and governance, and assess current compute, network, telemetry, tagging, and compliance context to identify gaps that could reduce CSW fidelity.

Phase 2: Solution Design and Planning

Define target CSW architecture, integrations, and labeling conventions, and produce the onboarding and supplemental telemetry plan to ensure ingestion and metadata quality across environments.

Phase 3: Build, Implement and Validate

Deploy CSW and required integrations, build ADM views with application teams, translate validated flows into intents and policies, run simulation/impact analysis, and progress approved scopes through monitor to enforce with controlled change windows.

Phase 4: Operations & Recommendations

Finalize operational processes, roles and responsibilities, and knowledge transfer, then deliver stabilization guidance and recommendations to expand segmentation across additional applications and zones.

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