Service Brief

Assessment

majentai

Cisco Secure Workload (CSW) Assessment

The Cisco Secure Workload (CSW) Assessment is a structured, executive-friendly engagement that validates prerequisites, surfaces risk, and aligns stakeholders on scope and success criteria. It produces a scored readiness scorecard and an execution-ready pilot roadmap. No deployment, agent rollout, or policy enforcement is performed.

Overview

This engagement is a short, low-risk readiness engagement designed to clarify the "why" and "where to start" for CSW, establish the foundational inputs required for a successful pilot, and deliver an implementation-ready plan for execution. It creates alignment before any tooling or rollout decisions are made, so teams can move into a pilot with clear scope, clean prerequisites, and shared governance.

- Define a focused, measurable pilot
- Confirm hosting footprint and inventory
- Validate telemetry and visibility approach
- Establish labels/metadata for policy
- Align operating model and governance

Business Outcomes

The CSW Assessment reduces implementation risk and accelerates time-to-value by validating prerequisites early, aligning governance, and creating a prioritized plan to move from discovery to controlled pilot execution. Readiness is scored across scope, inventory, visibility, metadata, integrations, segmentation model, and operating model to focus remediation where it matters most.

- Identify missing prerequisites and improve policy quality through clean metadata
- Accelerate pilot onboarding and validation and build cross-team alignment and ownership

At a Glance

Objectives

- Align stakeholders on pilot scope, success criteria, and decision rights
- Confirm feasibility of telemetry, integrations, and access prerequisites
- Produce a prioritized roadmap to execute a low-risk CSW pilot

Scope

- Pilot definition for 1–5 applications or a limited workload set
- Design-level readiness review
- Workshops and working sessions only; no agent rollout, no policy enforcement

Deliverables

- Readiness scorecard + top risks
- Prerequisites checklist + remediation plan
- Pilot definition + phased roadmap

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders on the "why," define pilot scope and success criteria, capture current-state inputs (inventory, visibility, metadata), and document decision rights and governance for simulate → monitor → enforce.

Phase 2: Solution Design and Planning

Define the target pilot approach, confirm integration and access prerequisites, establish the minimum labeling/taxonomy and mapping plan, and sequence remediation actions so onboarding can proceed without delays.

Phase 3: Build, Implement and Validate

Execute pilot preparation activities (prerequisites, access, labels), validate telemetry coverage and "good visibility," and produce the execution-ready pilot backlog and validation plan that will guide monitoring and controlled policy rollout.

Phase 4: Operations & Recommendations

Finalize the readiness scorecard and top risks, define the operating model (RACI, workflows, exceptions, rollback), and deliver a phased roadmap with clear next steps to move into implementation.

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