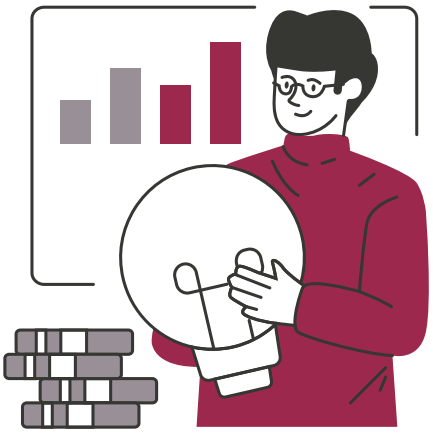
magentai

Why CSW?

Cisco Secure Workload (CSW) provides layered segmentation, from macro-level controls across environments to micro-level policies down to individual workloads. This multi-tiered approach significantly reduces the attack surface, helping protect critical applications and infrastructure with precision and control.



Why Magentai for CSW?

Magentai specializes in IaC (automation and self-service) and security focused around data-center and application platforms. Our ability to speak native application and cloud language allows us to bridge datacenter and security solutions finding the best fit between the two. Our comprehensive set of services encompass strategy, implementation, and enablement to ensure customers get the best build for their environment and feel comfortable while taking their applications to enforcement.

Proven Methodology

Magentai's structured approach ensures segmentation is done right from the start. From building, to validation and supporting long-term enforcement, we guide through every stage of the journey.

Build: Build foundational config & agent install.

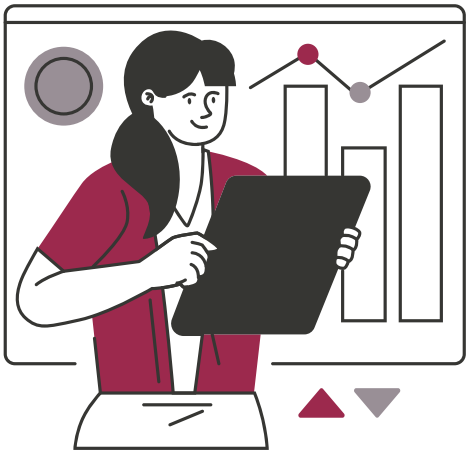
Analysis: Develop policy & pre-segmentation validation.

Discover: Application mapping leveraging machine learning algorithms.

Enforcement: Instantiate enforcement policy & post-segmentation functional testing.

Day 2 Support: Support customer team in continued enforcement and protection staying compliant with their segmentation mode.

magentai



Built for Results

- Reduce segmentation risk and complexity
- “Pilot to Co-Pilot” guided enablement
- Flexible engagement paths for every stage

Enforcement Factory

With hundreds to thousands of workloads, customers need a scalable way to reduce attack surfaces and enforce policy. That’s where our Enforcement Factory model comes in—designed to operationalize segmentation at scale through repeatable processes. Magentai leads the nation in Cisco Secure Workload deployments, bringing unmatched experience to every engagement.

Segment at Scale

- Reference architectures for key healthcare apps like EPIC and PACS.
- Unified policy for hybrid cloud segmentation across private and public environments.
- Accelerate deployment through repeatable, scalable segmentation patterns.

Network As a Sensor

- Simplify network snapshots by reducing tool sprawl
- Label traffic to identify normal vs. suspicious behavior
- Add context to telemetry to drive policy and enforcement decisions

Awards & Accolades

- 2019 & 2021 U.S. DSI Partner of the Year
- #1 DSI partner across multiple years
- 80+ Zero Trust deployments with 90%+ CSAT

magentai

Magentai 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.

magentai

Have Questions? We've Got Answers

When it comes to segmentation and security architecture, clarity is key. Below are answers to some of the most common questions we hear from teams navigating firewall strategy, policy control, and Cisco Secure Workload deployments.

Q **CAN I REPLACE MY FIREWALLS WITH CISCO SECURE WORKLOAD (CSW)?**

A CSW isn't a firewall replacement—it's a powerful complement. Firewalls remain essential for perimeter defense, while CSW extends protection deeper inside your environment through workload-level segmentation. By reducing the burden on your firewalls and introducing east-west visibility, CSW helps you achieve layered, comprehensive security.

Q **WILL I END UP WITH OVERLAPPING OR CONFLICTING POLICIES THAT WEAKEN SECURITY?**

A No. With CSW, policy intent is tightly controlled. We avoid broad, overly permissive rules like "any-any" and instead define precise, contextual policies. This minimizes the risk of unintended gaps and ensures that segmentation aligns with your security objectives.

Q **IF ACCESS IS ALREADY OPEN ON BOTH MY FIREWALL AND CSW, WHAT'S THE ADDED VALUE?**

A CSW goes beyond simple port and protocol control. It offers deep telemetry—providing visibility into the full process tree, identifying which application initiated the connection, and surfacing anomalies through behavioral baselining. This level of insight transforms raw access data into actionable security intelligence.

For more information or to engage our services, please contact us at info@magentai.com or visit https://magentai.com