majentai GUARDIANS

Segmentation Readiness Assessment

Turn Insight Into Action. Experience What Secure Feels Like.

This assessment is an adoption acceleration engagement targeting customers that are evaluating or planning to adopt a zero-trust segmentation initiative, or looking to optimize already deployed segmentation solutions.

Recommended Audience

- CISOs, SecOps, IT, and Network Teams
- Security & Infrastructure Leaders

Duration

- 30 Min Curation Call
- 4 Hours Onsite or Virtual Workshop
- 1 Hour Findings Presentation

Pre-Requisite

- Online Questionnaire

Outcomes

- Executive-Level Summary of Findings

Overview

This condensed & focused engagement equips security, infrastructure, and operations teams with advanced concepts and strategic approach to driving a Zero Trust Segmentation strategy. Real-world practitioners will discuss use cases, architectures, and case studies based on what is relevant to the customer. Participants will leave with a practical guide for segmentation that supports compliance, enhances resilience, and strengthens overall security posture and a recommended approach based on findings.

Areas of Focus (Select Two)

1. Perimeter Defense Architecture • *Securing Your Digital Boundaries*

Identify and secure entry and exit points in your enterprise. This session covers using firewalls, cloud security gateways, WAFs, and API gateways for layered network perimeter protection. Learn strategies for safe connectivity across clouds, data centers, and vendor systems.

2. Zero Trust Micro-Segmentation • *Eliminate Lateral Threat Movement*

Move beyond perimeter security with granular segmentation strategies that contain breaches and minimize blast radius. Apply micro-segmentation from network zones to process isolation to prevent compromised asset spread through your system.

3. Data-Centric Security Controls • *Protecting Your Most Critical Asset*

Data firewalls help users audit how many copies exist, their locations, related risks, and which systems access them. Learn how data firewalls provide classification, and visibility in protecting sensitive information.

4. Device Identity & Network Access Control • *Trust Through Verification*

Implement dynamic, policy-based network access that validates device posture and identity before granting connectivity. Learn enterprise NAC strategies including 802.1X, profiling, posture assessment, and automated threat response—ensuring only authorized, compliant devices access your network.

5. API Security & Authorization • *Securing the Modern Integration Layer*

APIs are the connective tissue of modern business—and a prime attack vector. Explore authentication protocols (OAuth 2.0, JWT), authorization frameworks, rate limiting, and threat protection strategies to secure your API ecosystem against abuse, data exposure, and unauthorized access.

6. AI Security Essentials • *Understanding Emerging AI Threats*

Get ahead of the AI security curve with practical insights into prompt injection, model manipulation, data poisoning, and AI-specific attack vectors. Learn defensive strategies for securing AI implementations and evaluating third-party AI services in your enterprise environment.

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