Battlecard

Uncover Zero-Trust Segmentation Opportunities

Modern IT environments are more complex than traditional perimeter security was built to handle. Cloud and hybrid operations often reduce visibility and make it harder to enforce consistent policy across a mix of tools, teams, and procedures. Zero Trust assumes breach, which shifts the focus from prevention alone to strong post-breach controls that help limit impact when an incident gets through. Micro-segmentation is a key control that reduces lateral movement, contains threats closer to critical assets, and gives security teams more time to detect, respond, and recover.

Challenges

In today's threat landscape, it's not if but when you get breached. Most enterprises get breached from exposed assets like web-servers and end-points. Additionally, hackers are continually leveraging human attack vectors via phishing and credential theft as well as exploiting vulnerabilities and moving laterally across the organization to steal valuable data, or disrupt business.

Solutions

- Hybrid Mesh Firewall
- Universal ZTNA
- Segmentation
- NAC/TrustSec

Segmentation Workshop
A guided, interactive workshop covering modern security architecture, best practices, and real-world use cases to align teams and define next steps.

Segmentation Readiness Assessment
Sales & adoption acceleration engagement targeting customers that are evaluating or adopting a Segmentation initiative.

Adoption Services
Professional services to design, implement, and integrate Cisco segmentation and hybrid-mesh-firewall solutions.

Guardian Support - Managed Services
Day-2 Support options to operate a Cisco-based zero-trust segmentation environment.

Questions to ask

- **Cybersecurity Framework Alignment**: "Are you aligning to a security framework today, like NIST, CIS, or ISO?"
- **Current challenges**: "What are the biggest gaps or pain points in your current security approach?"
- **Zero Trust + Segmentation**: "Where are you on Zero Trust, and do you use segmentation or micro-segmentation today?"
- **SecOps coverage**: "Do you have 24x7 monitoring and response today, or are you looking for an SecOps partner?"

Target Audience:

- Security leaders (CISOs, CIOs, IT Security Managers)
- Teams modernizing security in hybrid or multi-cloud environments
- Organizations with sensitive data and compliance requirements

Best fit for teams that need:

- A modern cybersecurity strategy focused on proactive protection and fast incident response
- Help designing or implementing Zero Trust and micro-segmentation
- Guidance through security and compliance requirements
- Faster outcomes while staying ahead of emerging threats
- A trusted partner to build and run a long-term security program

Terms to listen for:

- Zero Trust, Segmentation and micro-segmentation
- Managed Detection & Response (MDR)
- Security framework alignment (NIST, CIS, ISO)
- Compliance and audit readiness
- Advanced persistent threats (APTs)
- Tool sprawl and operational complexity

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

Advanced Persistent Threats (APTs)

What it is: Targeted, stealthy attacks designed to maintain access over time and achieve a specific objective.
Why it matters: Requires strong detection, segmentation, and response because attackers adapt and persist.
Listen for: “Nation-state,” “long dwell time,” “stealthy behavior,” “credential abuse,” “data exfiltration.”
Ask: “How do you detect suspicious behavior that blends in with normal user and system activity?”

Compliance and Regulations

What it is: Required standards and laws that govern how data and systems must be protected.
Why it matters: Drives security priorities, evidence needs, and timelines, with real business risk for noncompliance.
Listen for: “HIPAA,” “PCI,” “SOX,” “GDPR,” “CCPA,” “audit findings,” “evidence collection.”
Ask: “What compliance requirements are you accountable for, and what has been hardest to prove in audits?”

Cybersecurity Framework

What it is: A structured approach for managing security, such as NIST CSF, CIS Controls, or ISO 27001.
Why it matters: Creates a shared baseline for priorities, controls, and measuring maturity over time.
Listen for: “Maturity model,” “roadmap,” “controls,” “audit readiness,” “risk management.”
Ask: “Which framework or set of controls are you aligning to, and where do you see the biggest gaps?”

Micro-segmentation

What it is: Dividing environments into smaller, policy-controlled zones to restrict traffic and lateral movement.
Why it matters: Contains threats when something gets in and reduces blast radius.
Listen for: “Lateral movement,” “east-west traffic,” “app dependency mapping,” “hybrid visibility.”
Ask: “If one workload is compromised, how quickly can you contain it and stop it from spreading?”

Operational Complexity

What it is: The overhead of running security across many tools, environments, and legacy constraints.
Why it matters: Complexity creates gaps, slows response, and makes consistent policy enforcement difficult.
Listen for: “Tool sprawl,” “manual processes,” “integration issues,” “hybrid operations,” “too many consoles.”
Ask: “Where does complexity slow you down most today, visibility, policy consistency, or incident response?”

SecOps or Day-2 Support

What it is: 24x7 threat monitoring, investigation, and response support that combines tooling with human analysts.
Why it matters: Improves detection speed, containment, and consistency when internal staffing is stretched.
Listen for: “After-hours coverage,” “alert fatigue,” “SOC capacity,” “tool tuning,” “we need faster response.”
Ask: “Do you have 24x7 coverage today, and who owns containment and remediation during an incident?”

Zero Trust

What it is: A security model that verifies every user, device, and request before access is granted.
Why it matters: Reduces reliance on a trusted internal network and limits the impact of compromised credentials.
Listen for: “Remote access,” “identity,” “least privilege,” “conditional access,” “we assume breach.”
Ask: “What is your approach to verifying users and devices for every access request?”

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