

Zero Trust Security Posture Assessment

Majentai's Zero Trust Security Posture Assessment evaluates your current security ecosystem to identify architectural gaps, assess tool effectiveness, and recommend a roadmap to achieving Zero Trust maturity. We analyze across identity, devices, networks, applications, and data to ensure every user, device, and access request is continuously validated and verified.

Zero Trust Security Framework

A Zero Trust Security Posture is built on the principle of “never trust, always verify.” Instead of assuming implicit trust within the network perimeter, it enforces strict verification across every access point—regardless of user, location, or device. Our framework leverages five core pillars as the foundation for Zero Trust architecture.



Identity

An attribute or set of attributes uniquely describing a user or entity. Identity is the cornerstone of Zero Trust—ensuring only verified users and roles can access systems, with continuous validation and least privilege enforcement.



Device

Any physical or virtual hardware asset that can connect to a network. Devices must be authenticated, monitored for compliance, and continuously assessed for posture before being granted or maintaining access.



Network

Any physical, virtual, wired, wireless, public, or private communications medium. Zero Trust networks enforce micro-segmentation, limit lateral movement, and inspect traffic—both internal and external—to detect threats early.



Application

Any program or service residing on-premise, remotely, or in the cloud. Applications are protected through access controls, application segmentation, and runtime security policies that limit exposure and contain threats.



Data

Information generated, transferred, or stored by users, devices, or applications. Data security is enforced through classification, encryption, rights management, and continuous monitoring to ensure confidentiality, integrity, and availability.

Benefits

Strengthened Identity and Access Control

Ensure only verified users and devices gain access through MFA, RBAC, and continuous authentication.

Improved Internal Threat Detection

Reduce risk of lateral movement by increasing visibility and segmentation within internal traffic

Optimized Security Tool Performance

Identify alert fatigue, coverage gaps, and redundant functionality across endpoint, DNS, and network tools.

Enhanced Hybrid Security Coverage

Close visibility and enforcement gaps across both cloud and on-premise infrastructure.

Faster, More Accurate Incident Response

Improve detection, reduce noise, and automate triage through better tool integration and response workflows.

Core Deliverables

Strengthened Access Control: Enforce continuous authentication and least privilege access with identity- and role-based controls.

Improved Threat Detection: Increase visibility into internal traffic and reduce lateral movement through segmentation.

Reduced Alert Fatigue: Streamline alerts by eliminating redundancies and tuning detection across your security stack.

Enhanced Hybrid Coverage: Extend Zero Trust protections across cloud, on-premise, and legacy environments.

Accelerated Incident Response: Integrate tools and automate workflows to enable faster, more accurate response to threats.



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>