Service Brief

Assessment

majentai

Cisco Secure Networking Assessment

The Secure Networking Assessment is a structured evaluation designed to baseline infrastructure health, identify technical, operational, and security gaps, and prioritize modernization opportunities. Majentai reviews architecture, platforms, controls, and operations, then translates findings into a practical roadmap that improves resilience, scalability, and day-to-day manageability.

Overview

This assessment is an advisory engagement designed to evaluate network health and modernization priorities with clear findings and a path to phased improvement. The assessment validates infrastructure readiness across architecture, lifecycle, security, operations, and cloud edge while establishing the baseline required to reduce risk and guide future investment.

- Network architecture and topology review
- Hardware lifecycle and platform health
- Routing, switching, and segmentation readiness
- Cloud edge, SD-WAN, and wireless posture
- Operations, monitoring, and recovery controls

Business Outcomes

The Secure Networking Assessment reduces infrastructure and operational risk by converting fragmented network knowledge into a prioritized improvement plan. Majentai highlights gaps across resilience, security, and scale, and provides a roadmap for faster remediation, standardization, and better architectural decisions.

- Reduce hidden network and security exposure
- Improve resilience through prioritized remediation
- Standardize operations and configuration practices
- Enable modernization with clearer investment decisions

At a Glance

Objectives

- Establish a clear network health baseline
- Identify priority gaps, risks, and modernization needs
- Deliver business-aligned recommendations and sequencing

Scope

- Current-state review of core network domains
- Stakeholder workshops, documentation review, and technical analysis
- Prioritized roadmap spanning immediate through strategic improvements

Deliverables

- Executive summary presentation
- Comprehensive assessment report
- Updated topology and roadmap artifacts

Engagement Phases

Phase 1: Strategy and Discovery

Collect architecture, configuration, lifecycle, licensing, and operational inputs, and align with stakeholders on business drivers, pain points, service expectations, and growth assumptions that shape the assessment scope.

Phase 2: Solution Design and Planning

Evaluate topology, routing, switching, security, wireless, cloud edge, lifecycle, and management controls against best practices to identify gaps, single points of failure, vulnerabilities, and compatibility concerns.

Phase 3: Build, Implement and Validate

Translate technical observations into severity-based findings, highlight near-term remediation opportunities, and organize recommendations around business impact, operational feasibility, and modernization priorities.

Phase 4: Operations & Recommendations

Deliver the executive readout, detailed assessment outputs, updated documentation, and a phased roadmap that guides immediate remediation, short-term optimization, and longer-term architecture evolution.

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