

Cisco Secure Access MVP

Structured Engagement. Accelerated Value. Long-Term Success.

The Cisco Secure Access MVP engagement delivers a structured process that accelerates deployment while ensuring long-term security success. It aligns teams around defined objectives, provides expert-led guidance through each stage, and enables seamless integration with existing environments. The engagement is designed to streamline execution, reduce complexity, and establish a scalable foundation for secure access operations.

Use Cases

Cisco Secure Access empowers organizations to secure users, applications, and data across diverse environments. Whether enabling safe internet access, protecting sensitive information, connecting users to private and public apps, or monitoring digital experiences, the platform provides a comprehensive set of capabilities. These use cases demonstrate how Secure Access strengthens security posture while enhancing visibility, control, and user productivity.

Internet Access

Log and inspect all web traffic (HTTP/HTTPS) for full transparency, control, and protection. Forward traffic via IPsec tunnels, PAC files, or proxy chaining to enable visibility, URL and application controls, and advanced threat defense.

Private/Public ZTNA

Deliver app-specific, secure access to private apps in on-premises data centers or cloud/IaaS environments. Identity-aware proxy design enforces least privilege principles, denying access by default and granting access only when policies allow.

Data Loss Prevention (DLP)

Gain visibility and control over sensitive data with multimode DLP. Inspect data in-line, or use API-based analysis for data at rest in the cloud. Apply unified policies and reporting to streamline administration and meet compliance requirements.

DNS Protection

Block access to malicious or unwanted destinations at the DNS layer, across any port or protocol. Stop threats before connections are established to networks or endpoints.

VPNaaS

Secure access to all private apps, including those not supported by ZTNA. VPNaaS extends protection to non-web internet traffic, providing a cloud-delivered option for comprehensive secure connectivity.

Experience Insights (DEM)

Monitor endpoint, application, and network performance as users access resources. Automatically capture end-to-end experience data, optimize productivity, and speed incident resolution with AI-driven insights for proactive issue detection.

Key Benefits

Comprehensive Guidance:

Navigate complex deployments with expert mentoring for seamless execution.

Accelerated Deployment:

Achieve rapid implementation using best practices and proven methods.

Enhanced Security Posture:

Secure your environment with advanced features like ZTNA and threat analytics.

Tailored Solutions: Get a solution designed specifically for your infrastructure and goals.

Operational Efficiency:

Streamline processes and reduce costs through optimized resource use.

Knowledge Transfer: Equip your team with the skills and documentation for future management.

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



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.

Cisco Secure Access MVP

Proven Engagement Methodology

Our proven process and methodology are designed to ensure a smooth, efficient, and outcome-driven deployment. By combining structured workshops, collaborative working sessions, and clear milestones, we align business goals with technical execution at every stage. This approach provides transparency, accelerates time to value, and delivers measurable results while setting the foundation for long-term success.

Engagement Phases



Kickoff: Aligning teams on objectives, scope, and execution strategy. Establishes readiness, confirms logistics, and prepares for a smooth deployment start.

- Define success criteria, roles, and responsibilities
- Review kickoff deck and project plan
- Establish communication cadence and reporting structure
- Schedule Discovery Workshop and technical sessions



Discovery Workshop: Surfaces business goals, technical needs, and infrastructure considerations. Produces a tailored roadmap aligned to priorities.

- Deliver solution overview and align on value
- Gather security policies, integration needs, and constraints
- Define use cases and expected outcomes
- Validate readiness and finalize roadmap



Working Sessions: Surfaces business goals, technical needs, and infrastructure considerations. Produces a tailored roadmap aligned to priorities.

- Deploy and configure Cisco Secure Access components
- Conduct technical sessions with delivery and customer teams
- Resolve integration challenges in real-time
- Maintain structured progress tracking



Project Closeout: Transfers ownership through documentation, training, and handoff. Final feedback and recommendations support long-term success.

- Review outcomes and deliver final documentation
- Conduct platform training and Q&A
- Distribute CSAT survey and gather feedback
- Transition to Experience Team for support