Service Overview - Cisco Secure Access

OVERVIEW

This service delivers a structured deployment of Cisco Secure Access using BTA's SIMPLE methodology. The engagement provides secure, identity-based access to critical business applications — both internal (on-premises) and external (SaaS/cloud) — for all users regardless of location. It eliminates reliance on traditional VPN infrastructure, ensures a consistent security posture across the organization, and improves cyber insurance and compliance readiness.

KEY OUTCOMES

- Identity-based access to internal applications via ZTNA — replacing traditional VPN
- Secure web and SaaS application access via SSE — consistent protection regardless of user location
- Reduced reliance on legacy VPN infrastructure
- Improved cyber insurance readiness
- Documented architecture and operational handoff

IN-SCOPE CAPABILITIES

- Cisco Secure Access tenant configuration
- Identity provider integration
- ZTNA application onboarding (internal/private applications — per limits below)
- SaaS/cloud application policy configuration (per limits below)
- Secure Web Gateway (SWG) policy deployment
- Endpoint posture integration
- Pilot and production rollout
- Knowledge transfer and operational runbook

ENGAGEMENT SCOPE

Deployment Size	Users	Internal Apps	SaaS Apps	Duration
Small	<500	Up to 2	Up to 3	4–6 weeks
Mid-Size	500–1,000	Up to 4	Up to 6	6–10 weeks
Large	>1,000	>1,000	Custom	10–16 weeks

Internal Applications (ZTNA): Private, on-premises applications that previously required VPN access. Each requires connector deployment, access policy configuration, user group mapping, and testing.
SaaS/Cloud Applications: Externally hosted business applications (e.g., Salesforce, ServiceNow) requiring individual CASB policy configuration or application-specific access controls beyond standard SWG category policies.

SWG Policy: Standard URL category filtering, malware/threat protection, DNS security, and SSL decryption with a standard exception list are included. Custom DLP policies, multiple per-group policy sets, and Remote Browser Isolation (RBI) configuration are additional scope.

General internet security is covered through SWG category-based policies and is not subject to the application limits above. Additional applications beyond scope may be addressed as change requests or follow-on engagements.

BTA Service Overview - Cisco Secure Access

BTA'S SIMPLE METHODOLOGY

START — **Project initiation and alignment** - Kickoff meeting, scope and success criteria validation, stakeholder alignment, application prioritization - Deliverables: Project plan, kickoff documentation, agreed application scope

IMMERSE — **Environment discovery and requirements gathering** - User/device/identity assessment, application inventory, current VPN/proxy/security review, pilot scope definition, access model determination (agent-based vs. agentless/BYOD) - Deliverables: Current state summary, pilot scope, application onboarding priority list

MAP — **Architecture and policy design** - Secure Access architecture design, ZTNA segmentation model, SWG policy framework, SaaS application policy design, rollout planning - Deliverables: Architecture diagram and design document

PROVE — **Pilot validation of design and policies** - Tenant configuration, identity and endpoint integration, ZTNA connector deployment, pilot application onboarding, policy testing and tuning, success criteria validation - Deliverables: Pilot results report and validated configuration

LAUNCH — **Production deployment** - Production rollout planning, expanded application onboarding, organization-wide user rollout, final policy implementation - Deliverables: Production deployment completion

EVOLVE — **Optimization and operational transition** - Policy refinement, operational documentation and runbooks, knowledge transfer sessions, executive closeout - Deliverables: Operational runbook and final project report

CUSTOMER RESPONSIBILITIES

- **Provide access to required systems and stakeholders**
- **Supply user and application inventories**
- **Identify and prioritize applications for onboarding (within scope limits)**
- **Support pilot communications and change management**
- **Provide required Cisco licensing**

EXCLUSIONS

- Applications beyond the stated scope limits
- Custom application development or modification
- Legacy VPN decommissioning (migration in scope; decommission is advisory only)
- Cisco ISE integration (available as add-on; may impact hours and timeline)
- Cisco SD-WAN integration
- Enterprise-wide endpoint agent deployment (architecture and pilot in scope; mass rollout is customer responsibility)

sales@GoBTA.com 678-951-8980 GoBTA.com

Schedule A Call