

Security Whitepaper — BISTEC ServiceNow Copilot Gateway (Hartley)

Reviewer-facing summary for Microsoft Marketplace certification and for a customer's IT security team. Distilled from [docs/architecture/security-compliance-agent-accelerator.md](#) , [docs/architecture/zero-trust-assessment.md](#) , and [infra/marketplace/REVIEW.md](#) .

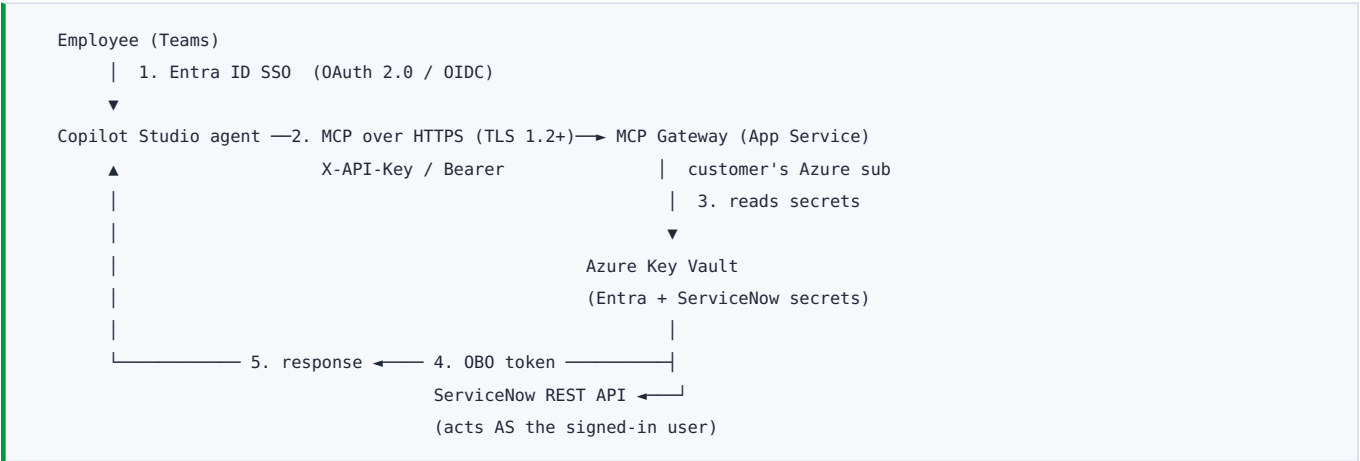
Status: draft — requires BISTEC security sign-off before submission.

Publisher: BISTEC Global · Product: Hartley — ServiceNow IT-Support Agent · Deployment model: Customer-hosted Azure Managed Application

1. Architecture in one paragraph

Hartley has two components. The **Copilot Studio agent** (distributed via AppSource) is the conversational front end. The **MCP Gateway** (this Azure Application offer) is an Azure App Service that translates Model Context Protocol calls into ServiceNow REST API calls. The gateway deploys entirely into the **customer's own Azure subscription** — BISTEC operates no shared multi-tenant service and holds no customer data or credentials.

2. Data-flow diagram



1. User authenticates to the agent with **Entra ID SSO** — never anonymous.
2. Agent calls the gateway over **HTTPS (TLS 1.2 minimum)**, authenticated with an API key.
3. Gateway reads ServiceNow + Entra secrets from **Key Vault** at runtime.
4. Gateway performs an **on-behalf-of (OBO)** token exchange so ServiceNow actions run as the signed-in user — preserving ServiceNow's own RBAC and audit trail.
5. Result flows back to the user. No conversation content is persisted by the gateway.

3. Identity & access

Control	Implementation
User authentication	Microsoft Entra ID SSO (OIDC), enforced — anonymous access disabled
Service authentication	API key (X-API-Key /Bearer) on the MCP endpoint; rotated before production
ServiceNow authorization	Per-user OAuth on-behalf-of — no shared service identity for user actions
Least privilege	ServiceNow service account limited to itil , catalog , knowledge roles
Managed identity	App Service uses managed identity for Key Vault access where supported

4. Secret management

- All secrets — Entra client secret, ServiceNow OAuth client secret, gateway API key — are stored in **Azure Key Vault** provisioned in the customer's subscription.

- Secrets entered in the deployment wizard use `PasswordBox` and go **directly into Key Vault**; they are **never written to ARM deployment history** or the offer package.
- No secrets are hardcoded in the container image or configuration (verified by compliance checks AGT-007 and FLW-105).

5. Data residency & protection

- All resources deploy to the **Azure region the customer selects** (reference deployments use `australiacentral`). Data does not leave that region by design.
- Encryption in transit (TLS 1.2+) and at rest (Azure platform encryption on Key Vault, storage, and App Service).
- The gateway is **stateless** — it does not store tickets, conversation history, or PII; it proxies to ServiceNow, which remains the system of record.

6. Network security

- Public endpoint is HTTPS-only; the MCP path requires authentication even when OAuth is disabled for testing.
- Optional **VNet integration** and **custom domain** are offered as deployment inputs for customers with private-network requirements.
- NSG/firewall rules follow least-privilege (ARM-TTK certified, 49/49 tests passing).

7. Governance & compliance

The Copilot Studio agent passes an **8-phase, 73-point compliance validation** before deployment, covering (abridged):

- **Agent level:** Entra SSO enforcement, content moderation (Medium/High), no hardcoded secrets, PII handling, locked-down customizability.
- **Environment level:** active DLP policy, approved-maker security groups, guest access disabled, audit logs to Log Analytics.
- **Flow level:** approved connectors only, secure inputs/outputs, authenticated HTTP actions, error handling and timeouts.
- **Organizational level:** documented data residency, incident-response plan, compliance framework mapping.

Full control matrix: [docs/architecture/security-compliance-agent-accelerator.md](#) .

8. Shared-responsibility summary

Layer	Owner
Azure infrastructure (App Service, Key Vault, App Insights)	Customer's subscription
Gateway application code + updates	BISTEC (publisher)
ServiceNow instance, data, and user roles	Customer
Identity (Entra tenant, SSO, consent)	Customer
Secret values	Customer (stored in their Key Vault)