Enhancing Snowflake Security Using Private Azure Infrastructure

Private Cloud Security for Enterprise Data

A US based design and manufacturing company with over 6,000 employees relied on Snowflake for enterprise analytics but needed a secure internal chatbot without public internet exposure.

We built a fully private Zero Trust environment on Microsoft Azure, integrating Azure OpenAI securely with Snowflake.

CLIENT BACKGROUND

A United States based design and manufacturing company with over 6,000 employees specializes in high precision industrial components. The organization uses Snowflake for enterprise analytics across engineering, finance, and operations to manage and analyze data.

BUSINESS VALUES

Faster Data Access: Analytics became 60% faster, enabling employees to make quicker decisions.

Reduced Security Risk: Exposed attack surface reduced by 70%.

Cost and Efficiency Gains: Optimized costs while maintaining fully private internal traffic.

PROBLEMS

- **Sensitive Data at Risk:** Important design and manufacturing was under risk of exposure through public internet connections.
- **Strict Compliance Pressure:** The company had to meet NIST, CMMC, ISO 27001, and SOC 2 security rules.
- **No Safe Internal Data Access:** No secure internal system to connect Azure services with Snowflake privately.

SOLUTIONS

- **Private and Secure Environment:** All services were configured with private endpoints, ensuring no public exposure and fully isolated network traffic.
- **Controlled User Access:** Entra ID authentication, conditional access, MFA, and RBAC ensured only authorized users could access data.
- **Data Protection and Monitoring:** Implemented encryption, secure key management, query logging, and monitoring, and maintained data safety and activity visibility.
- **Compliance and Governance:** Aligned with NIST, CMMC, ISO 27001, SOC 2, and Zero Trust principles for audit readiness.

TECHNOLOGIES

FUTURE SCOPE

The company now has faster, secure, and fully private data access, with future steps adding RAG, Microsoft Purview, anomaly detection, and stronger data classification for deeper control and oversight.