Security Whitepaper

Comprehensive overview of SummitView security architecture

1. Overview

SummitView is a Power BI monitoring and intelligence platform that provides complete visibility into semantic model refreshes, usage analytics, workspace inventory, capacity utilization, data quality, and gateway monitoring.

This document describes the security architecture, data handling practices, and compliance posture of SummitView to support your IT security review process.

2. Security Principles

- Metadata Only: SummitView collects operational metadata — never actual report data or business information
- Read-Only Access: All Power BI API calls use read-only permissions. SummitView cannot modify anything in your environment
- Outbound Only: No inbound network connections are required. All data flows are outbound HTTPS from your network
- No Credential Storage: The agent uses OAuth 2.0 tokens with automatic refresh. No passwords or secrets are stored on disk
- BYOK AI: AI analysis features use your own API keys. Data goes directly from your browser to your AI provider
- Tenant Isolation: Each organization's data is fully isolated in the database with row-level security policies

3. Data Collection

SummitView collects the following metadata for monitoring purposes:

+ Workspace names and IDs
+ Dataset names, refresh times, and durations
+ Report names and view counts
+ Gateway names, types, and connection types
+ Capacity utilization metrics (CPU, memory)
+ User activity events (who viewed what report, when)
+ Row counts per table (for anomaly detection)
+ Asset governance metadata (criticality, lifecycle, owners)

SummitView NEVER collects:

x Actual report data, visualizations, or business information
x Database contents, query results, or row-level data

- x User passwords, tokens, or stored credentials
- x DAX queries, M-code, or SQL statements
- x File contents, attachments, or embedded images
- x Personal data beyond name/email from Azure AD profile

4. Authentication & Authorization

Web Application Authentication:

- Microsoft SSO via Azure AD (multi-tenant)
- OAuth 2.0 authorization code flow with PKCE
- No SummitView-specific passwords — enterprise identity only
- Role-based access: Owner, Admin, Member, Viewer

Agent Authentication:

- MSAL-based OAuth with Azure AD
- Delegated permissions (works on behalf of signed-in user)
- Automatic token refresh — no credentials stored on disk
- Signed-in user must have Power BI Admin role for admin API access

5. Infrastructure Security

- Hosting: Vercel (SOC 2 Type II certified)
- Database: Supabase PostgreSQL (SOC 2 Type II certified)
- Encryption at Rest: AES-256 for all stored data
- Encryption in Transit: TLS 1.2+ for all network connections
- Email: Resend (transactional email for alerts)
- Payments: Stripe (PCI DSS Level 1 certified)
- Database Access: Row-level security (RLS) policies enforce tenant isolation

6. AI Security (BYOK)

SummitView's AI analysis features use a Bring Your Own Key (BYOK) model:

- SummitView does not operate any AI infrastructure
- AI queries go directly from your browser to your configured AI provider (OpenAI, Azure OpenAI)
- No data passes through SummitView servers for AI analysis
- You control which AI provider to use and which API key is configured
- AI features are optional and disabled by default

7. Deployment Options

Option A: Cloud Connect (Service Principal)

- No software installation required
- Service principal configured in Azure AD with read-only Power BI API access
- SummitView cloud collects data directly via Power BI Admin APIs

Option B: Agent + Cloud Connect (Recommended)

- Lightweight Windows service installed in your environment
- Provides enhanced monitoring: per-table refresh timing, row counts, Pro workspace support
- Outbound HTTPS only — sends metadata to SummitView cloud
- Code-signed installer available; MSI deployment via SCCM/Intune supported

8. Compliance

Current Security Controls:

+ HTTPS/TLS encryption everywhere
+ OAuth 2.0 authentication (no password storage)
+ Tenant data isolation via row-level security
+ GDPR-ready data handling
+ Role-based access control
+ SOC 2-aligned practices (infrastructure providers are SOC 2 certified)

Compliance Roadmap:

- SOC 2 Type II certification (planned)
- ISO 27001 (future consideration)
- GDPR Data Processing Agreement (DPA) available on request

9. Security Contact

For security questions, vulnerability reports, or to request a security review:

Email: security@summitview.app

Web: summitview.app/security