Security Document for AI File Pro

Introduction

This document outlines the security measures embedded within the AI File Pro product, focusing on its interactions with local databases, Azure Computer Vision, and Azure OpenAI. It describes how these integrations ensure data privacy and security throughout the document processing lifecycle, based on the product's use of Azure AI services for intelligent file organization and analysis.

Security Measures Overview

Secure Connection to Azure Services

AI File Pro establishes secure connections to Azure services, following Microsoft's best practices for network security. Key elements include:

- **TLS Encryption**: All communications are secured using Transport Layer Security (TLS) 1.2 or higher, ensuring data in transit is encrypted and protected from interception.
- **Authentication Protocols**: Utilizes OAuth 2.0 and Azure Active Directory for secure authentication and authorization, preventing unauthorized access to Azure resources.
- **Network Isolation**: Employs Azure Virtual Networks (VNets) and best practices for perimeter security to isolate traffic and reduce attack surfaces.learn.microsoft.com

Azure Computer Vision Security

Image Processing and Security Measures

AI File Pro utilizes Azure Computer Vision (part of Azure AI Vision) for OCR and image analysis, extracting text and analyzing document content. The following security measures are in place:

- **Data Encryption in Transit and at Rest**: Data is encrypted during transmission via HTTPS and TLS 1.2. During processing, data is temporarily encrypted in Azure Storage.
- **Access Management**: Authentication via API keys and Azure AD ensures only authorized requests are processed.
- **Data Minimization and Isolation**: Only required image data is sent, processed in the customer-specified region, with no sharing across customers.learn.microsoft.com
- **Data Retention Policies**: Input data and results are not retained post-processing for Image Analysis; for OCR, they are deleted within 24 hours to prevent long-term exposure.

Azure Computer Vision processes images for features such as text extraction and object detection, ensuring privacy by not storing facial templates or using data for improvement without explicit consent.

Azure OpenAI Security

Handling of AI-Generated Content

AI File Pro integrates Azure OpenAI for generating file names, folder structures, and content summaries. Security measures include:

- **Data Encryption**: Prompts and responses are encrypted in transit and at rest using AES-256, with options for customer-managed keys.
- **User Data Isolation**: Customer data is logically isolated, not shared with others, and not used for training models without permission.learn.microsoft.com
- **Monitoring and Logging**: Interactions are monitored for abuse, with optional modified monitoring where data is not stored
- **Data Retention Policies**: Uploaded data can be deleted anytime; for abuse monitoring, data is stored up to 30 days if enabled, but not used beyond detection purposes.learn.microsoft.com

Azure OpenAI handles AI-generated content for document classification and organization, maintaining privacy by processing within customer-specified geographies.

Compliance with Regulations and Standards

AI File Pro, through its Azure integrations, adheres to key data security and privacy regulations:

- **GDPR**: Supports data residency and processing commitments, ensuring compliance for EU users.
- **HIPAA**: Azure services offer compliance for health data, though customers must configure accordingly (note: Computer Vision may not be fully HIPAA-compliant for all features).
- **ISO/IEC 27001**: Aligns with Azure's information security management certifications.learn.microsoft.com
- **Other**: Follows Microsoft Products and Services Data Protection Addendum for broad compliance.learn.microsoft.com

Local Data Security

The local data and database for AI File Pro are stored in the user's AppData folder. This location leverages Windows' built-in file system protections to enhance data security and isolation. Key features include:

- Per-User Data Isolation: The AppData folder is part of the individual user profile, ensuring that data is segregated between different users on the same machine. Other users cannot access this folder without administrative privileges or explicit permission changes.learn.microsoft.com+2 more

- File System Permissions: Protected by NTFS access control lists (ACLs), the folder grants complete control to the owning user and SYSTEM account, with restricted access for others. Administrators may have elevated permissions, but standard users are limited to their profiles.
- Hidden Directory: The AppData folder is hidden by default in Windows File Explorer, reducing the risk of accidental discovery or tampering by users.
- System-Level Protections: Windows applies additional safeguards, such as User Account Control (UAC) and integration with Windows Defender, to prevent unauthorized modifications or malware access within user profiles.
- Data Encryption: All data stored locally is encrypted using industry-standard encryption protocols (e.g., AES-256).
- Access Controls: Role-based access controls (RBAC) restrict user permissions, ensuring that only authorized personnel can access sensitive data.

Conclusion

AI File Pro provides a secure framework for document processing by keeping core operations local and leveraging Azure's robust security for cloud-based AI features. Encryption, minimal retention, and compliance measures collectively prevent data exposure and ensure privacy.

