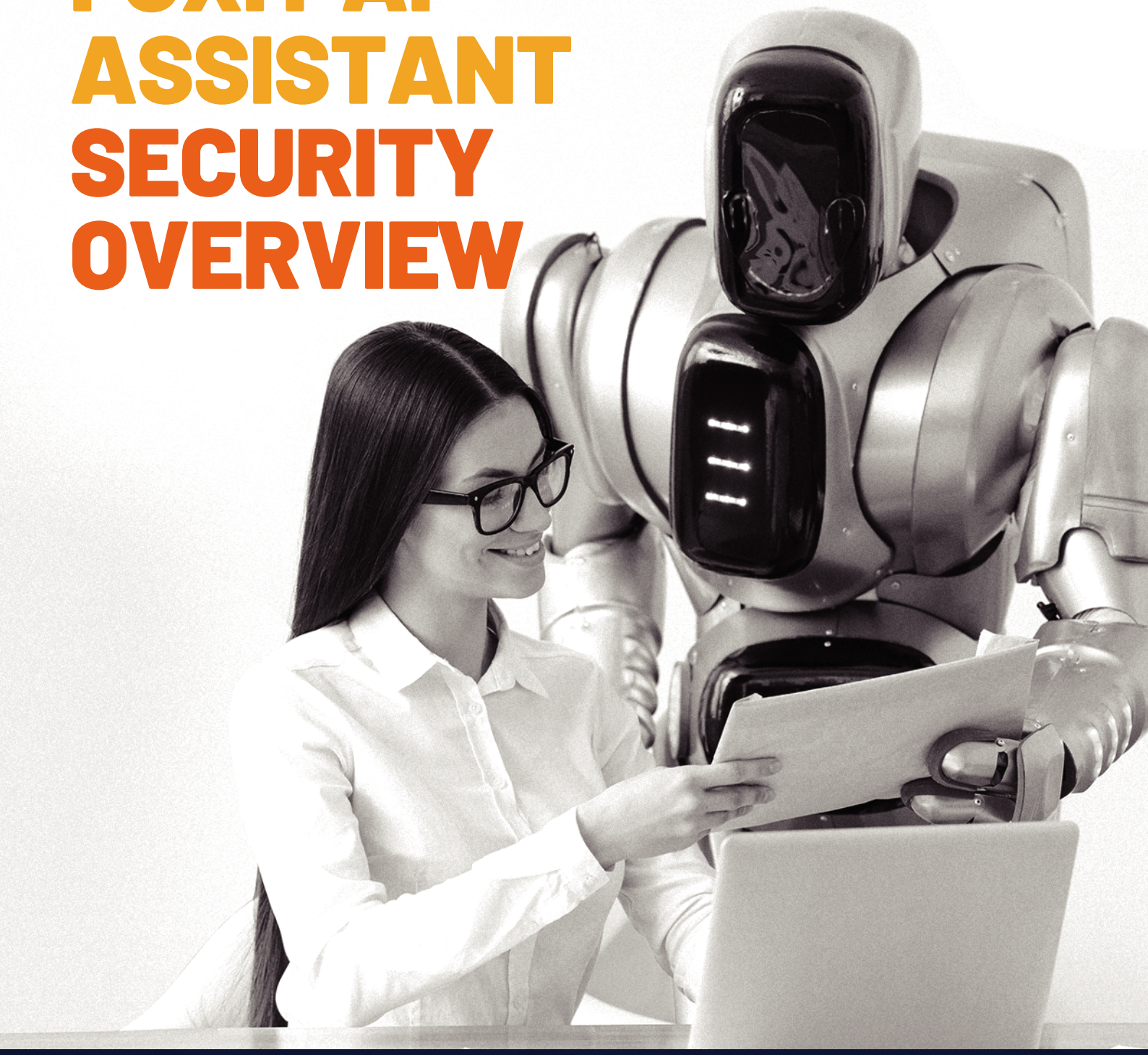
FOXIT AI ASSISTANT SECURITY OVERVIEW

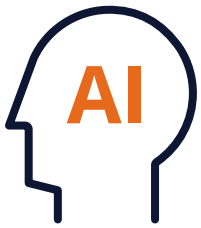


WHITE PAPER

TABLE OF CONTENTS

FOXIT SECURITY

Foxit Software places a strong emphasis on security to protect its software and user data. We follow secure software development practices, including code reviews and vulnerability assessments, to identify and address potential security vulnerabilities. Encryption is utilized to safeguard sensitive data during transmission and storage. Secure document handling features, such as password protection and digital signatures, are implemented to prevent unauthorized access and tampering. User authentication mechanisms, including password-based authentication and multi-factor authentication, ensure that only authorized individuals can access specific features or perform certain actions.



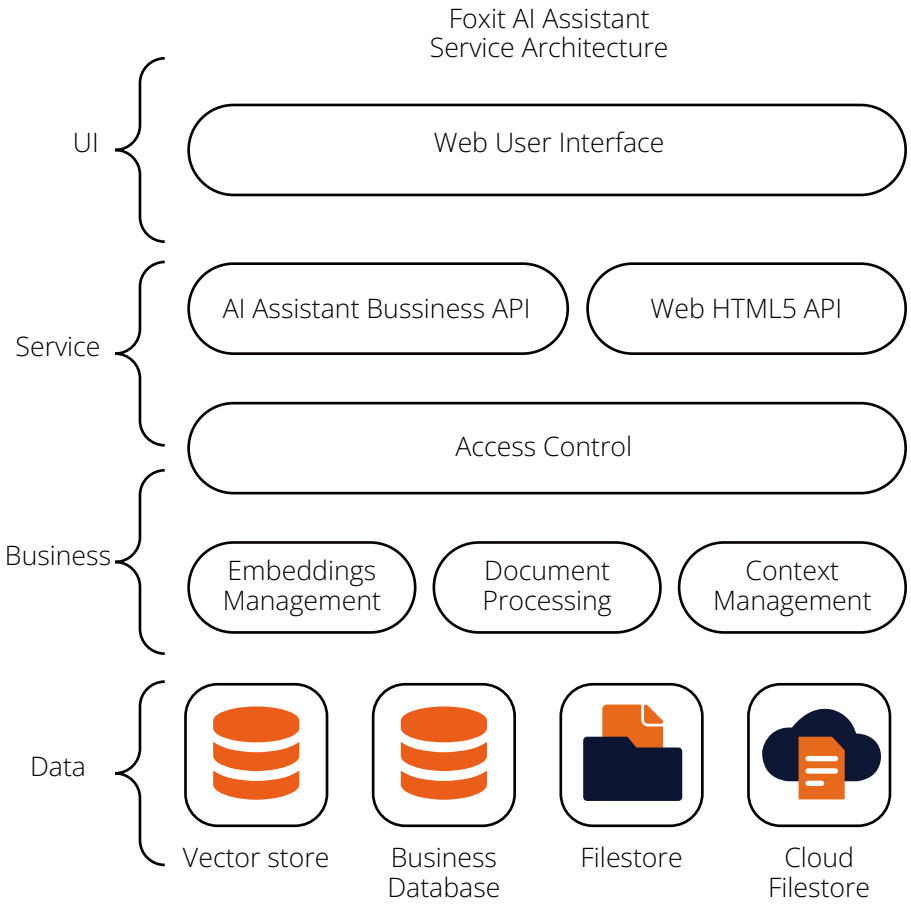
ABOUT FOXIT AI ASSISTANT

Foxit AI Assistant integrated with Azure OpenAI, which is an innovative solution that helps users understand and interact with documents more effectively. By combining advanced artificial intelligence technology with powerful language processing capabilities, the Foxit AI Assistant integrated with Azure OpenAI offers a range of functions that enhance productivity and streamline document comprehension.

- Document Summary - The OpenAI summary service uses artificial intelligence to generate a concise and accurate summary of a given text input.
- Document Re-write - The OpenAI rewrite service uses machine learning to automatically paraphrase or rewrite text while maintaining its original meaning. This service is free up to 100 pages per user per month.
- Content Translation - Translating selected text into corresponding languages. Maximum 2000 characters per prompt, 50 prompts per user per day.
- Document Q&A - Have a conversation with PDF and answer user questions based on PDF content, 50 prompts/questions per user per day.
- Content Explanation - AI-powered feature that provides concise explanations and definitions for selected text.
- Spelling and Grammar Correction - AI-powered feature that automatically detects and corrects spelling and grammar errors in your content.
- SMART PDF COMMANDS - Delegate tasks to our AI Assistant for efficient document processing.

And other more features.

FOXIT AI ASSISTANT SERVICE ARCHITECTURE



The objective of the design of the Foxit AI Assistant service architecture is to provide highly reusable, secure, and scalable service components. With the aim of achieving this overarching goal, we have implemented a layered approach, encompassing the following tiers: user interface layer, service layer, business layer, and data layer.

The user interface layer presents the AI Assistant window in a web page format, receives user questions or commands, and returns responses to the user.

The service layer provides service APIs for application invocation and includes user access control functionalities. It includes the following:

- AI Assistant Business API: Provides business logic APIs for managing user tokens, document summarization/enhance writing/translation, and more.
- Web HTML5 API: Provides communication interfaces between web components and the application end.
- Access Control: Offers user access control capabilities, defining which resources users can access and their permissions for accessing those resources.

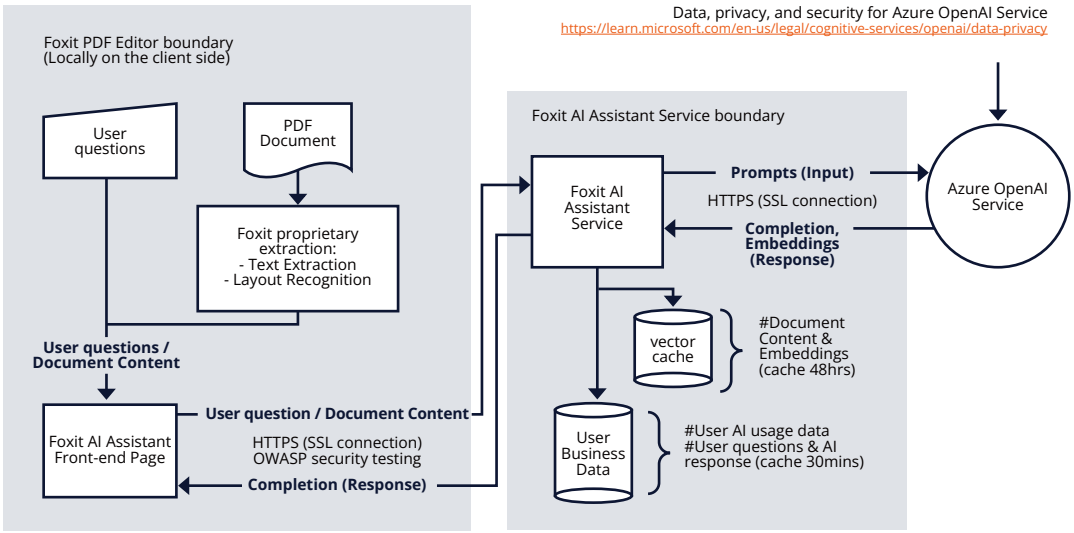
The business layer encompasses document data processing, vector management, and chat session context management, among others. It includes the following:

- Embeddings Management: Manages vector data for text, including updates, similarity search, and comparisons. An embedding is a relatively low-dimensional space into which high-dimensional vectors can be translated.
- Document Processing: Identifies and extracts content from documents, segments text content, and more.
- Context Management: Manages the context of user sessions.

Lastly, the data layer comprises the repositories and storage mechanisms used by the AI Assistant. It incorporates components such as vector databases, business databases, local document storage, and cloud document storage. These components play a crucial role in efficiently managing and accessing the data required for the AI Assistant's operations.

By implementing this architectural design, the Foxit AI Assistant service ensures disaster backup and recovery capabilities, guaranteeing the availability and stability of the services provided to users. Additionally, the architecture emphasizes observability, enabling real-time monitoring of the service's health. In the event of any service interruptions or anomalies, the system can swiftly identify and resolve issues, minimizing any disruptions experienced by users.

FOXIT AI ASSISTANT SECURITY ARCHITECTURE



The subsequent steps outline the workflow within the Foxit AI Assistant Security Architecture:

1. **User enters a question and submits it**
2. **PDF document preprocessing**

    a) **Text extraction.** Parse and extract text content from all pages of the PDF document. Based on the token length limitations, the text content of the document may be divided into multiple segments.

    b) **Layout recognition.** Using the layout recognition engine developed by Foxit, recognize the document's layout information and extract the following document details:

        1. Tables
        2. Article titles
        3. Paragraphs
        4. Other information

3. **The front-end web page (which is embedded in Foxit PDF Editor) calls the Foxit AI Assistant Service API, passing the user input question and the preprocessing data of the PDF document as the parameters to Foxit Server.**

4. **The Foxit AI Assistant Service then calls the Azure OpenAI service and retrieves the results from Azure OpenAI.**

    a) The user input and PDF document preprocessing data will be processed with embeddings calculation and similarity search. The final matching results are sent to the Azure OpenAI API as prompts.

    b) The preprocessing results of the PDF document and the embeddings will be cached in the vector database to speed up subsequent calls.

    c) Return the results obtained from Azure OpenAI to the Front-end and display them on the Front-end Page.

5. **Data, privacy, and security**

    a) The development of Foxit AI Assistant complies with OWASP, a rigorously secure programing framework. And it took anti-virus, penetration, and vulnerability tests before releases.

    b) All web APIs are called via the HTTPS protocol, including calls to the Foxit AI Assistant Service API and Azure OpenAI API. This ensures the security of document and user's data transmission.

    c) The databases used in the service (User Business Data/Vector Store) are not exposed to the public. They are protected by a firewall and can only be accessed within the internal network.

    d) User prompts (inputs), completions (outputs) and User document content are not stored permanently in Foxit AI Assistant Service, for performance reason,

        i. User prompts (inputs) & completions (outputs) might be stored in the database for a maximum of half an hour before being deleted,

        ii. and User document content might be stored in the database for a maximum of 48hrs before being deleted.

    e) The Azure OpenAI service used by the AI Assistant has its own security standards. For details, refer to: https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy?context=%2Fazure%2Fai-services%2Fopenai%2Fcontext%2Fcontext.

FOXIT SECURITY OVERVIEW

Foxit Security is composed of these forms:

- Document Security: Ensure that information within a document is not compromised.
- Application Security: Guard against and/or quickly deal with any security related problem associated with a Foxit product.
- Cloud Security: Ensure your data is safe over the internet.
- Deployment and Administration security: By offering related capabilities and configuration options.

DOCUMENT SECURITY

Foxit PDF Editor allows document authors to create PDF documents and apply various security measures, including encryption, access control, digital signatures, and AI based redaction (the permanent removal of content). The ease of use and power of these features provided by Foxit PDF Editor allows both individual users and organizations to effectively keep their information private and confidential.

APPLICATION SECURITY

In addition to document security, we at Foxit recognize that the software itself can be a target of attacks, so we take our application security very seriously. As such, we have long adopted measures and processes that are leading industry best practices to ensure our application security, and have also introduced features and capabilities in the software itself so that users can further protect themselves in specialized situations.

CLOUD SECURITY

Cloud services provided by Foxit enhance the capabilities and user experience of the Foxit End User Productivity solution. These services are constantly monitored for availability, performance, as well as security.

- **Data Center Security**
  All Foxit cloud services are managed by our trusted cloud service provider, Amazon Web Services (AWS), which is an ANSI tier-4 data center, and maintains verify strict controls around data center access, fault tolerance, environmental controls, and security. Only approved, authorized Foxit employees, cloud service provider employees, and contractors with a legitimate, documented business area are allowed access to the secure site in Virginia, USA, Frankfurt, Germany and Montreal, Canada.
- **Data Encryption and Privacy**
  Foxit cloud services are designed with privacy and security as a high priority. All information transmission between the users and the Foxit cloud services are fully secured with 256-bit AES encryption over the HTTPS transport protocol.

  Foxit employees and trusted vendors only access customer data to perform certain business and support functions, or as required by law.
- **Off-Grid Operation**
  Foxit offers users and organizations the option to operate the software in complete “off grid” mode, where no cloud service access will be performed by the software installed by users. This capability offers additional deployment and operational flexibility for organizations with high level of security needs.

DEPLOYMENT AND ADMINISTRATION

By offering security related capabilities and configuration options, such as disabling JavaScript execution, cross-domain resource access, and enabling “off grid” operation, Foxit has made its software more robust against attacks, and can reduce or eliminate the need for out-of-band security updates, as well as lowering the urgency for regularly scheduled updates. This leads to operational flexibility, as well as lowered Total Cost of Ownership (TCO), especially in large organizations with high level of requirements for security.

CONCLUSION

Foxit offers a best-in-class level of security protection tailored to meet the diverse needs of users with varying requirements for PDF functions, as well as organizations of different sizes and industries. We acknowledge the sensitivity of your information and workflow, emphasizing the utmost protection they demand. With Foxit, you gain a trusted vendor committed to not only delivering uncompromising PDF software but also ensuring its security across all facets in accordance with industry best practices.
For more information on Foxit security, please go to the Foxit Security Center.

Foxit
39355 California Street, Suite 302
Fremont, CA 94538, USA

Sales: 1-866-680-3668
Support: 1-866-693-6948
Or 1-866-MYFOXIT

Support Center
www.foxit.com