Product Guideline

Kinsmen AI
Security Features

Rev: 2

Date: 30 May 2024

KINSMEN AI

Table of Contents

Introduction

In today's evolving digital landscape, robust security measures are paramount for protecting sensitive information and ensuring compliance with international standards. This Kinsmen AI Security Features document outlines the comprehensive security solutions integrated within the solution, leveraging Microsoft 365 and Azure services. This document provides a detailed overview of the solution design, core security features, adherence to international security standards, and the benefits these bring to safeguarding data and operations. By adopting these advanced security protocols, the solution not only enhances the protection of its clients' data but also ensures seamless and secure user experiences.

Solution Design

The solution is built around Microsoft365 and Azure services. The back-end systems use serverless technologies including CosmosDB, Functions, Logic Apps, EventHub and SignalR messaging. The Azure OpenAI Co-Pilot stack is included in the back-end services and is integrated into the Kinsmen Group solution using OpenAI Large Language Models.

Front-end systems access data through a managed and documented REST API connecting to back-end microservices. Front-end user interfaces are coded in React.js and include MS365, Teams and Outlook .Net web parts built based on Microsoft guidelines. The user interface follows the Microsoft FluentUI guidelines, also supporting a mobile interface.

The solution is designed to be easily and regularly updated with new features and fixes and will constantly evolve to address new security concerns and take advantage of new facilities in the MS365 and Azure environments.

Security benefits of this approach and environment are described below:

Security Features

1. **Identity and Access Management (IAM):** Azure Entra ID provides identity services that can be seamlessly integrated with Microsoft 365 applications. This ensures secure authentication and authorization.

2. **Multi-Factor Authentication (MFA):** Both Azure and Microsoft 365 support MFA, adding an extra layer of security.

3. **Data Encryption:** Azure services, including CosmosDB support encryption at rest and in transit. Microsoft 365 also supports encryption for data at rest and during transmission.

4. **Monitoring and Auditing:** Azure Monitor and Azure Security Center provide comprehensive monitoring, logging, and alerting capabilities. Microsoft 365 also has its own security and compliance center for similar functionalities.

5. **Serverless Security:** Azure Functions and Logic Apps are secured using Entra ID and can also be set to run within a Virtual Network, further isolating them.

6. **API Security:** Azure API Management is used by the Kinsmen Group solution to manage and secure REST APIs, including rate limiting, IP restrictions, and API key management.

7. **Data Loss Prevention (DLP):** Microsoft 365 has built-in DLP features that can be extended to SharePoint and Teams. SharePoint includes a 2 stage recycle bin.

Azure Cosmos DB automatically takes backups of your data at regular intervals. The automatic backups are taken without affecting the performance or availability of the database operations. All the backups are stored separately in a storage service, and those backups are globally replicated for resiliency against regional disasters.

For Microsoft 365, Microsoft provides a variety of backup options for different services. For example, Exchange Online uses Exchange Native Data Protection (NDP) which provides multiple copies of data in different locations

8. **EventGrid Security**: EventGrid supports message authentication through SAS tokens or key authentication.

9. **Network Security:** Azure provides various network security features like Azure Firewall, Network Security Groups (NSGs), and Virtual Networks to isolate resources.

10. **Compliance Tools:** Both Azure and Microsoft 365 offer a set of tools to help with compliance reporting and data governance, such as Azure Policy and Compliance Manager in Microsoft 365.

11. **Data Segregation:** Every customer has a separate database in the Kinsmen Group solution, this has the following security advantages:

Data Isolation:

Reduced Blast Radius: If one database is compromised, the impact is limited to the data within that specific database, rather than affecting all customer data.

Fine-Grained Access Control: You can set up more specific roles and permissions on a per-database basis. This is particularly useful in multi-tenant environments where different customers may have different data access needs or restrictions.

Compliance and Regulatory Benefits:

Data Sovereignty: For customers subject to specific data residency requirements, having separate databases can make it easier to place data in a geographic location that complies with local laws.

Easier Auditing: When customer data is separated, it can be easier to audit access and changes to each database, which can be crucial for compliance with regulations like GDPR, HIPAA, or CCPA.

Operational Security:

Resource Governance: You can allocate resources like throughput and storage on a per-database basis, which can prevent a security incident affecting one customer from depleting resources that are critical for others.

Encryption Keys: CosmosDB allows for customer-managed keys for encryption at rest. Different databases can use different keys, providing an additional layer of security.

Backup and Restore: In the event of a data issue or security incident, having separate databases can make it easier to restore data for a single affected customer without impacting others.

Query and Network Security:

Limited Scope for Query Attacks: If an attacker gains access to execute arbitrary queries, the damage is limited to a single database rather than potentially affecting all customer data.

Network Isolation: You can set up Virtual Network Service Endpoints or Firewall rules on a per-database basis, providing additional network-level security.

Monitoring and Alerting:

Focused Monitoring: With separate databases, you can set up more targeted monitoring and alerting policies, making it easier to spot anomalous behavior that could indicate a security issue.

Data Usage Patterns: Monitoring is simplified when each database corresponds to a single customer, as deviations from normal behavior are easier to spot.

International Security Standards

1. ISO/IEC 27001: Both Azure and Microsoft 365 are compliant with this standard, which is one of the most widely recognized security standards.
2. CIS Benchmarks: Azure complies with the Center for Internet Security benchmarks.
3. NIST: Azure services align with NIST cybersecurity frameworks.
4. GDPR: Both platforms offer tools to help with GDPR compliance.
5. HIPAA: Azure and Microsoft 365 offer features that can support HIPAA compliance, although the responsibility is shared with the customer.
6. FedRAMP: For U.S. government customers, both platforms are FedRAMP compliant.
7. PCI DSS: Azure is compliant with Payment Card Industry Data Security Standard, which is crucial for applications dealing with financial transactions.
8. Microsoft Azure also conforms to ISO 27017:2015, ISO 27018:2019, SOC 1 Type 2, SOC 2 Type 2 and SOC 3 Type 2.