ALICE™
RECEPTIONIST

Cloud Security Overview

March 15, 2016

Table of Contents

ALICE Cloud Security Overview

ALICE Cloud Services are hosted on the Microsoft Azure cloud infrastructure. Alice cloud databases, services and applications take advantage of built in encryption for both data at rest and in transit. Data stored on the ALICE Cloud infrastructure is encrypted both at rest and in transit. Azure threat detection allows ALICE Cloud Services to monitor and detect anomalous database activities indicating potential security threats to the Alice cloud databases. Data stored on the Azure cloud a broad set of industry standards including ISO 27001, SOC 1, SOC 2 and FedRAMP.

Azure compliance meets a long list of international, regional and industry specific standards. The security compliance framework includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis to achieve certificates and attestations. Microsoft Azure offers an extensive list of certifications for all in-scope services which are inherited by the ALICE Cloud services and data.

Microsoft Azure Platform

Microsoft Azure provides cloud services for a wide range of enterprise and government customers. The core of Microsoft Azure provides four primary functions on which customers build and manage virtual environments, applications, and associated configurations.

Microsoft, with its unique experience and scale, delivers these services to many of the world's leading enterprises and government agencies. Today, the Microsoft cloud infrastructure supports over 1 billion customers across our enterprise and consumer services in 140 countries and supports 10 languages and 24 currencies. Drawing on this history and scale, Microsoft has implemented software development with enhanced security, operational management, and threat mitigation practices, helping it to deliver services that achieve higher levels of security, privacy, and compliance than most customers could achieve on their own.

Microsoft shares best practices with government and commercial organizations and engages in broad security efforts through the creation of centers of excellence, including the Microsoft Digital Crimes Unit, Microsoft Security Response Center, and Microsoft Malware Protection Center.

Compliance

By being hosed on the Microsoft Azure Cloud platform, Alice Receptionist's cloud infrastructure inherits the benefits of Microsoft's investment in infrastructure security.

Microsoft invests heavily in the development of robust and innovative compliance processes. The Microsoft compliance framework for online services maps controls to multiple regulatory standards. This enables Microsoft to design and build services using a common set of controls, streamlining compliance across a range of regulations today and as they evolve in the future.

Microsoft compliance processes also make it easier for customers to achieve compliance across multiple services and meet their changing needs efficiently. Together, security-enhanced technology and effective compliance processes enable Microsoft to maintain and expand a rich set of third-party certifications.

Azure meets a broad set of international as well as regional and industry-specific compliance standards, such as:

- ISO 27001
- FedRAMP
- SOC 1
- SOC 2

Azure's adherence to the strict security controls contained in these standards is verified by rigorous third-party audits that demonstrate Azure services work with and meet world-class industry standards, certifications, attestations, and authorizations.

Azure is designed with a compliance strategy that helps customers address business objectives and industry standards and regulations. The security compliance framework includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis to achieve certificates and attestations. Microsoft Azure offers the following certifications for all in-scope services:

- CDSA
- CJIS
- CSA CCM
- EU Model Clauses
- FDA 21 CRF Part 11
- FedRAMP
- FERPA
- FIPS 140-2
- HIPAA
- IRAP
- ISO/IEC 27018
- ISO/IEC 27001/27002:2013
- MLPS
- MTCS
- PCI DSS
- SOC 1 and SOC 2
- TCS CCCPPF
- UK G-Cloud

Data Encryption

DATA AT REST

Data at rest stored on the ALICE Cloud infrastructure is encrypted using Azure SQL Database Transparent Data Encryption.

Azure SQL Database transparent data encryption helps protect against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups, and transaction log files at rest.

TDE encrypts the storage of an entire database by using a symmetric key called the database encryption key. In SQL Database the database encryption key is protected by a built-in server certificate. The built-in server certificate is unique for each SQL Database server. If a database is in a GeoDR relationship, it is protected by a different key on each server. If 2 databases are connected to the same server, they share the same built-in certificate. Microsoft automatically rotates these certificates at least every 90 days.

DATA IN TRANSIT – Available in production: April 1st 2016

Data in transit between the ALICE Cloud infrastructure and ALICE deployed applications is transferred securely using Secured Socket Layers (SSL) protocol.

Secure Socket Layer (SSL) encryption is the most commonly used method of securing data sent across the internet. It is the standard security technology for establishing an encrypted link between a web server and a browser. SSL ensures that all data passed between the ALICE cloud servers and applications remain private and secured.

Threat Detection

Alice cloud infrastructure use Azure Threat Detection to detect anomalous database activities indicating potential security threats to the Alice cloud database.

Threat Detection provides a layer of security, which enables ALICE staff to detect and respond to potential threats as they occur by providing security alerts on anomalous activities.

For example, Threat Detection detects certain anomalous database activities indicating potential SQL injection attempts. SQL injection is one of the common Web application security issues on the Internet, used to attack data-driven applications. Attackers take advantage of application vulnerabilities to inject malicious SQL statements into application entry fields, for breaching or modifying data in the database.

Documentation

Certifications, Trust Documents and supporting documents are available upon request.