CloudLink Security

Frequently Asked Questions (FAQ)

Summary:	This document addresses some commonly asked questions about CloudLink security
Posted Date:	October 18, 2021
Audience:	Mitel Sales, Partners, and Customers
Revision Version:	1.4
Revision Reason:	Updated publication

Overview

The CloudLink platform is Mitel's next-generation cloud platform. CloudLink provides a rich suite of application-enabling services including Identity and Access Management (IAM), chat, presence, notifications, workflow, media services, and Short Message Service (SMS).

CloudLink itself is not a product or application that a customer can purchase. Rather, CloudLink has implemented application-enabling microservices that are used by Mitel to build and enhance the applications that are purchased and deployed by its partners and customers.

The CloudLink platform is built on the market leading Amazon Web Services (AWS) cloud computing platform which provides enterprise level uptime and stability, multi layered security, and data protection and privacy. Details around some of the most frequently asked questions (FAQ) related to the security and data processing of the CloudLink platform are provided below.

In which geographic regions is CloudLink deployed?

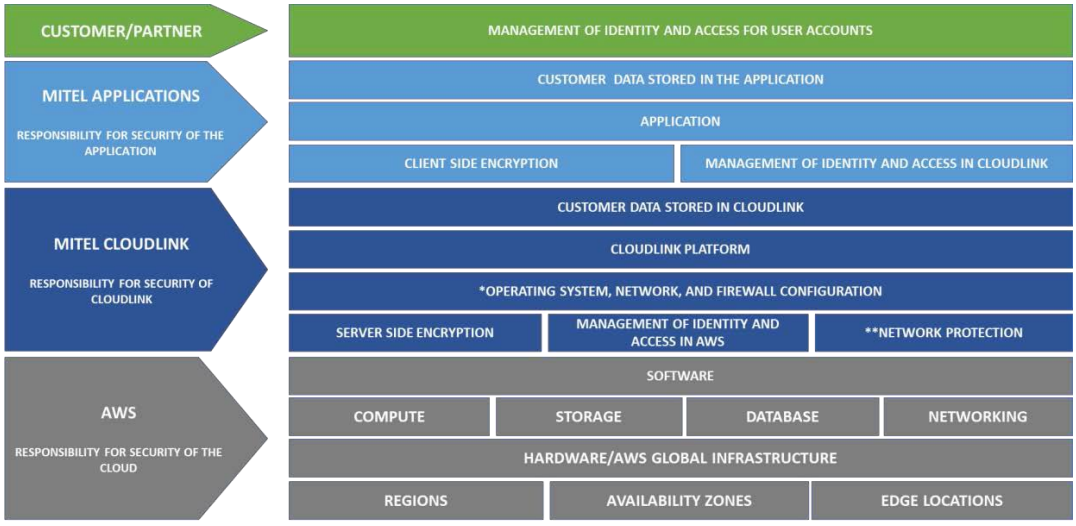
The CloudLink platform is deployed on AWS infrastructure within North America, Europe, and Asia-Pacific regions and availability zones. For information regarding AWS regions and availability zones, see https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html. The CloudLink platform builds on AWS' scalable, highly available, and redundant architecture. User data is retained within the home service cloud for each CloudLink account. Please note that due to the dynamically elastic nature of the platform, the service may be delivered from different physical locations within an AWS Availability Zone.

What are the roles AWS, Mitel, and the Customer play in the protection of customer data?

CloudLink platform security is based on a layered security model in which security roles lie with:

- the underlying infrastructure provider (i.e.., AWS)
- the CloudLink Platform and its suite of services
- the Mitel Applications which leverage the CloudLink Platform services
- and the customer

The figure below explains the separation of roles and responsibilities.



Note:
* responsibility moves down to AWS in a serverless computing model
** Majority of the responsibility moves down to AWS and CloudLink is responsible for Internet access, monitoring, and logging in a serverless computing model

The CloudLink platform is a microservices based architecture built on AWS. The CloudLink platform adheres to the best practice recommendations from AWS, in terms of configuration and deployment of the services, which include the categories of networking, monitoring, logging, and alerting to ensure state of the art protection. This includes enabling encryption in the foundation services provided by AWS and enforcing encryption when transmitting data between the customer and the CloudLink platform (i.e. data in transit).

A principle of “least privilege” access is also enforced in the platform’s serverless deployments t o ensure Mitel employee access is limited based on their role and permissions.

The CloudLink platform provides services to Mitel applications, which enables the applications to provide a rich set of Unified Communications features to the customer. While it is the responsibility of the CloudLink platform to protect customer data stored in the platform, Mitel applications are responsible for protecting customer data stored in the application, and the customer is responsible for management of their user access and user accounts.

Does the CloudLink platform provide Identity and Access Management (IAM)?

The CloudLink platform simplifies access and account management by providing an Identity and Access Management (IAM) service based on Open ID Connect 1.0 and federated single sign-on (SSO) using SAML 2.0.

How does the CloudLink platform secure data in transit?

Data is encrypted from the customer’s endpoint to the AWS foundation services, which the CloudLink platform uses for the microservices deployed in a serverless configuration. For the microservices deployed using AWS Elastic Computer Cloud (EC2), encryption is enforced between the customer’s endpoint to the Virtual Private Cloud (VPC). Transport Layer Security (TLS 1.2) is used creating a tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption.

How does the CloudLink platform secure data at rest?

The CloudLink Platform uses industry standard AES 256-bit encryption when encrypting data at rest.

How are encryption keys managed?

The CloudLink platform leverages AWS Key Management Service (KMS) and AWS owned Customer Master Keys (CMKs). The CloudLink platform does not support the import of a customer’s own encryption keys.

How does the CloudLink platform secure internal communication and APIs?

APIs provided by the CloudLink platform for use by Mitel applications, are secured via the CloudLink IAM framework using full encryption during transport. Encryption of data in transit is described above.

Does CloudLink perform regular data backups for service continuity?

The CloudLink platform uses services provided by AWS to perform regular database backups.

Who has access to customer data?

The CloudLink platform follows the guidelines and best practices defined by AWS to ensure that the infrastructure is configured correctly to ensure data isolation at the infrastructure level. Infrastructure configurations are monitored and changes in infrastructure are audited to protect against tampering.

Two levels of Identity Access Management (IAM) are implemented in the CloudLink Platform. The first is an AWS native IAM used at the AWS infrastructure level with strict Role Based Access Control (RBAC), Multi Factor Authentication (MFA), and a principle of least privilege. Only Mitel employees with a job function (e.g., Tier 3 support) that requires access to the production environment have access to the configuration and deployment of the AWS infrastructure, and the permissions of their accounts are limited to the performance of their duties. The second is an IAM service provided natively by the CloudLink platform to ensure data access is isolated to the properly credentialed individuals (e.g., account administrators). While CloudLink provides the infrastructure and the security of the infrastructure for IAM, it is also the responsibility of the partner/customer to configure their user accounts appropriately to limit access to customer data.

In the case of Mitel partners, the partner creates the initial CloudLink account for each customer which holds the synchronized users from the client application. User information in the CloudLink account is typically managed natively from the client application and synchronized with CloudLink. The partner or customer admin also has the capability of managing a user's username and email address from directly within CloudLink. However, it should be noted that an individual customer's user data is not visible to anyone other than that customer. Logs and analytics related to the customer are restricted to a limited set of members of the Mitel DevOps, Operations, Security Team, and Product Support team as required to support customer incidents and on-going product improvements.

Do customers have access to logs and/or analytics?

The CloudLink platform does not provide customers with any access to platform logs and/or analytics. Platform logs and analytics are restricted to a limited set of members of the Mitel DevOps, Operations, Security Team, and Product Support Team as required to support customer incidents and on-going product improvements. However, applications built on the CloudLink platform may provide logs and analytics to the customer, as deemed appropriate by each application.

Does CloudLink maintain an audit trail of changes made to the platform?

The CloudLink platform follows the best practice guidelines of AWS for auditing using AWS CloudWatch for logging within the CloudLink platform and AWS CloudTrail, AWS Config, and AWS GuardDuty for auditing changes within the infrastructure. The CloudLink Platform does not provide customers access to audit logs, except when required by law.

For how long is your data retained in CloudLink?

Unless your organization has otherwise agreed with Mitel, metadata and content are retained for as long as your organization has a CloudLink account and is entitled to use the CloudLink service.

Does CloudLink have a privacy policy?

CloudLink does not a have a separate privacy policy. To understand how Mitel applications using CloudLink process personal information, please see Mitel's Application Privacy Policy available at https://www.mitel.com/en-ca/legal/mitel-application-privacy-policy.

What security policies does the CloudLink platform follow?

Mitel security policies cover areas such as information security, incident response, logical access to production, change management, and product support. These internal policies are reviewed and approved at least annually. Employees, interns, and contractors are notified of updates to these internal policies through

ongoing security training, by email, and/or via our security policies intranet page.

- Information Security: Policies pertaining to user and CloudLink Platform information, with key areas including device security, authentication requirements, data and systems security, employee use of resources guidelines, and handling of potential issues.
- Physical Security: Measures taken to maintain a safe and secure environment for people and property at Mitel sites; AWS is responsible for maintaining the physical security of their infrastructure.
- Incident Response: Requirements for responding to potential security incidents, including assessment, communication, and investigation procedures.
- Logical Access: Policies for securing CloudLink systems, user information, and CloudLink information, covering access control to corporate and production environments.
- Physical Production Access: Procedures for restricting access to the physical production network, including management review of personnel and de-authorization of terminated personnel.
- Change Management: Policies for code review and managing changes that impact security by authorized developers to application source code, system configuration and production releases.
- Support: User metadata access policies for our Support Team regarding viewing, providing support, or for taking action on accounts.

What certifications/compliances does the CloudLink platform have?

While the AWS infrastructure that CloudLink is built on has numerous certifications and compliances, the CloudLink platform itself is currently in the process of becoming compliant to PCI DSS, SOC2, and HIPAA.