CloudLink Chat Security

Summary:	This document addresses some commonly asked questions about CloudLink Chat security
Posted Date:	September 3, 2020
Audience:	Mitel Sales, Partners, and Customers
Revision Version:	1.2
Revision Reason:	Updated publication

Table of Contents

Purpose

Mitel takes security and safety seriously in protecting the confidentiality, integrity, and availability of customers' data. Mitel recognizes security as a crucial aspect of our systems. The purpose of this whitepaper is to provide Mitel customers with an overview of the security of the Mitel CloudLink Chat service.

Introduction

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 Chat service is one example.

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. The CloudLink platform follows AWS best practices and guidelines (See https://aws.amazon.com/security). This ensures proper isolation and protection of the customers' data at the highest degree while also providing enterprise level uptime and stability, multi layered security, and data protection and privacy.

Definitions

Only acronyms specific to this document are listed here.

Terms/Acronym	Definition
AES	Advanced Encryption Standard
AWS	Amazon Web Services
IAM	Identity and Access Management
RBAC	Role Based Access Control
SDLC	Software Development Life Cycle
SSE	Server-Side Encryption
TLS	Transport Layer Security

Shared Responsibility Model

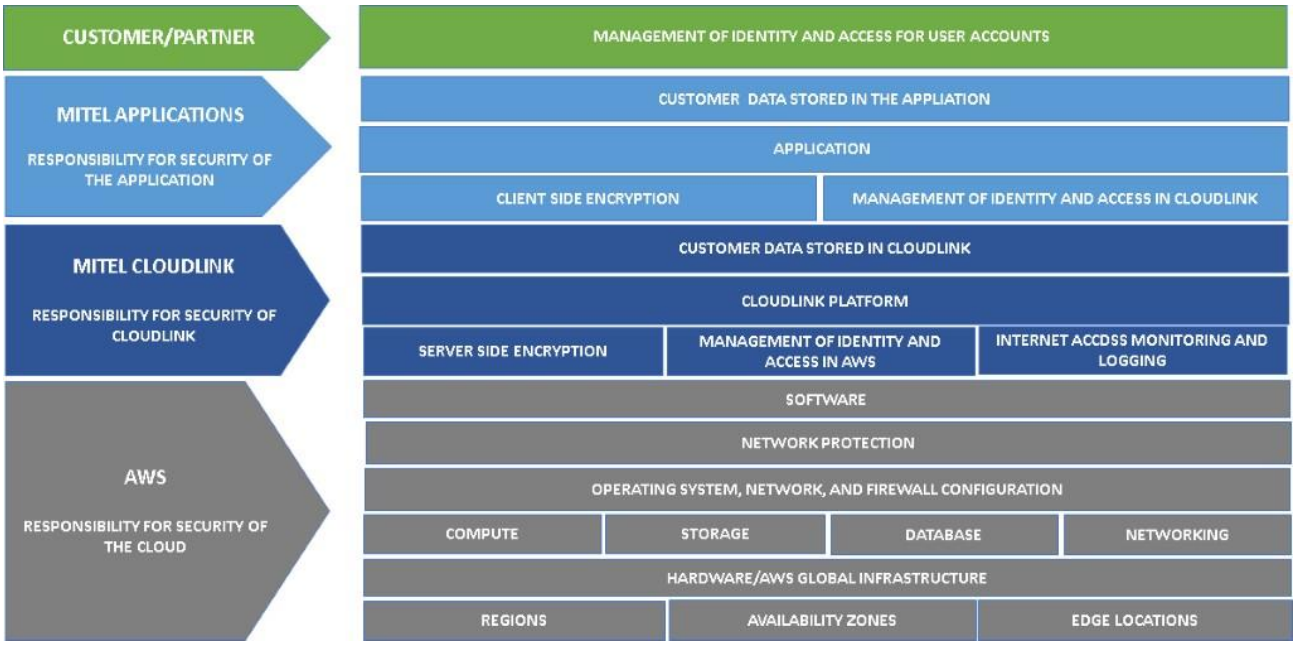

Figure 1: Shared Responsibility Model

Security is a shared responsibility and this shared responsibility model is also applicable to applications that utilize Mitel's CloudLink platform. Security responsibilities are shared between the infrastructure provider (AWS), Mitel (CloudLink platform and Mitel applications), and the Customer.

Figure 1 provides more details on the responsibilities of each entity. AWS is responsible for protecting the AWS Cloud infrastructure and foundation services right down to the physical level. CloudLink is responsible for the security related to the microservice code, the storage, isolation, and accessibility of data used by the microservice, and identity and access management to the AWS foundation services which the microservices use. The CloudLink platform provides services to Mitel applications, which enables the application to provide a rich set of Unified Communications features to the customer. While it is the responsibility of the CloudLink platform to protect the 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.

Identity Access

Identity Access Control is also a shared responsibility between the CloudLink platform, Mitel Applications, and the customer.

The CloudLink platform's responsibility is ensuring access to the AWS foundation services used by the CloudLink platform are secured and restricted to Mitel employees and limited to their job function. The best practices employed include the use of AWS Organizations, Role Based Access Control (RBAC) for limiting access to job functions of personnel, Multi-Factor Authentication for accessing AWS infrastructure, and dedicated security accounts in AWS (to ensure security events are monitored by the correct personnel).

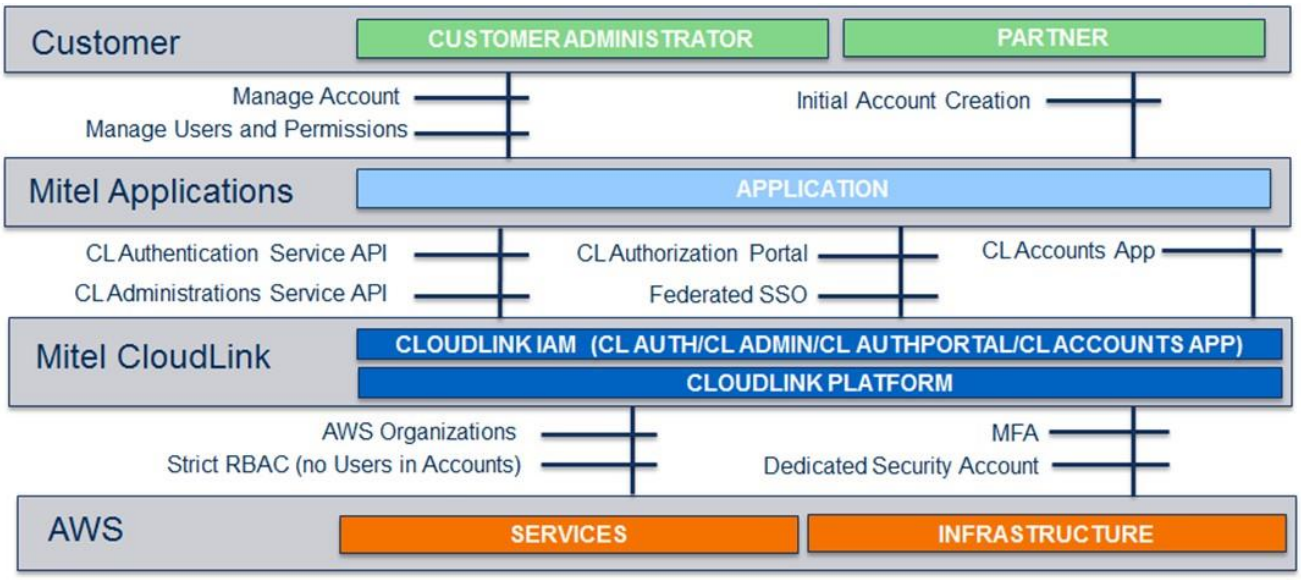

Figure 2: Identity Access Management in the Shared Responsibility Model

Mitel applications ensure that identity and access for the accounts and users of that application are properly reflected within the CloudLink platform. The Mitel application performs these functions through secure APIs provided by the CloudLink Identity Access Management (IAM) solution which ensures access to the services and data is isolated to the appropriate account and limited to the responsibilities of the users defined by the customer.

The CloudLink IAM solution is an open solution supporting Open ID Connect 1.0 with support for federated single sign-on (SSO) using SAML 2.0. The CloudLink IAM solution offers a common login portal (CloudLink Authorization Portal) which the Mitel application can redirect to for its SSO requirements.

The partner/customer is responsible for managing the account, users, and permissions within the Mitel Application.

NOTE: *A Mitel partner is required to initially create the customer account in CloudLink from the CloudLink Accounts Application which can be launched via MiAccess.*

Data in Transit

To protect data in transit, encryption is enforced between the client and the services provided by the CloudLink platform. This includes desktop, mobile, web, and API. The CloudLink platform uses Transport Layer Security (TLS 1.2) for data transfer, with Amazon CloudFront creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. More information on how CloudFront secures data can be found in the "Secure Content Delivery with CloudFront" document located at https://aws.amazon.com/security/security-resources.

Data at Rest

The CloudLink Chat Service code runs on a serverless deployment using AWS S3 Elastic Search foundation services to store data. Server-Side Encryption (SSE) protects data at rest. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced

Encryption Standard (AES-256), to encrypt your data (See the "Securing Data at Rest with Encryption" document located here https://aws.amazon.com/security/security-resources/).

Keys are managed using the AWS Key Management Service (KMS) following the best practices provided by the provider. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated (https://aws.amazon.com/kms/)

Deletion of Customer Data

Customer account data stored by the CloudLink Chat service is deleted when the customer account is removed from the CloudLink platform.

Data Retention

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.

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.

Security of Chat Content

Files and links in Chat are not executed by the CloudLink Chat service, so the Chat service is not impacted by malicious content. The Chat service does not access the content uploaded by the user and is not able to perform virus/malware scans directly on the user's data. As stated above, security is a shared responsibility and the validity of the content lies with the customer. It is highly recommended that the customer installs the appropriate antivirus/malware software on their devices as a general security guideline.

Geographic Availability

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.

Customers can review the status of Mitel's CloudLink services by navigating to https://status.mitel.io.

Information Security

The CloudLink Team uses an information security framework and regularly reviews and updates security policies, provides security training, performs application and network security testing, monitors compliance with security policies, and conducts internal risk assessments.

Mitel Security Policies

Mitel security policies encompass 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.

Policy	Definition
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. AWS datacenter physical security is managed by Amazon.
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 for, or taking action on accounts.

Employee Policy and Access

Mitel employee access to the CloudLink production environment is maintained by a central directory and authenticated using a combination of strong passwords and Multi Factor Authentication. Access to the environment is restricted to the AWS Console and AWS CLI and is limited to Mitel engineering teams requiring access as part of their duties. IAM administration of the AWS foundation services is tightly controlled and limited to a small number of administrators. Authorized employee access is removed upon employee status being changed (e.g. change in role or employment status) with the CloudLink administration team being part of the Human Resources (HR) notification process.

Mitel maintains separate development and production environments and access is limited to each based on the authorized employee's role. In addition, Mitel's internal policies require employees accessing production and corporate environments to adhere to best practices for the creation and storage of secret access keys required to access the AWS infrastructure.

Employee on-boarding and off-boarding policies require, security policy acknowledgement, communicating updates to security policy, and non-disclosure agreements.

The CloudLink platform employs technical access controls and internal policies to prohibit employees from accessing customer user files. 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.

The CloudLink Development and Operations Teams receive on-going training with up to date security best practices and governances. Automated security testing is integrated within the Software Development Life Cycle (SDLC) along with more in-depth manual vulnerability testing on a periodic basis.

Access Monitoring

All access to the CloudLink platform and the AWS services which the platform uses are logged based on time of day, IP address, log-in IDs. CloudLink logs are only accessible by authorized Mitel personnel.

The CloudLink platform staff routinely review several system parameters including access logs to ensure there are no malicious access attempts into the secured environment.

Network Security

By utilizing Amazon Web Services serverless implementation for the CloudLink Chat Service, the solution makes use of AWS network security, by default, through the shared responsibility model provided by AWS.

In addition to the inherent security capabilities of AWS (DDoS mitigation, data encryption etc.), the CloudLink platform adheres to the recommendations and best practices provided by AWS in architecture and deployment, to ensure no variances creep in that can compromise the security of the solution.

The CloudLink Team diligently monitors security events and anomalies to ensure any attacks on the CloudLink platform is contained and mitigated as quickly as possible. As highlighted elsewhere in this document access to the production environment is restricted to a limited set of approved CloudLink personnel.

Change Management

The CloudLink platform is supported by a formal **Change Management Policy** to ensure that all application changes have been authorized prior to implementation into the production environments. The process is enforced using an automated code, build, and deploy pipeline.

Source code changes are initiated by developers that would like to make an enhancement to the application or service. Code reviews are enforced, which include examination of possible security issues prior to merging and deploying the changes to a staging environment. CloudLink Service primes are identified for each CloudLink service and act as gatekeepers to ensure that security standards are met for submissions to be deployed to the staging environment and subsequently, later into the production environment. This includes verifying the necessary code review changes are implemented, and that Quality Assurance (QA) testing has passed the necessary criteria.

Once the changes are properly soaked in the staging environment, the respective CloudLink Service primes initiate the changes through an automated code, build, and deploy pipeline where the same rigorous testing that was done in staging is performed again in production, before going live with the change. The serverless implementation of the CloudLink platform supports a rollback mechanism to ensure service is quickly recovered in the event of a critical issue escaping into live production.

The infrastructure for the CloudLink Chat Service is provided by AWS through a serverless implementation. The deployment and configuration are using the best practice defaults provided by AWS to ensure the security and integrity of the solution is set to the highest standard.

Through the shared responsibility model provided by AWS for serverless deployments, AWS is responsible for the security of the foundation services AWS provides and the infrastructure, including operating systems, firewalls, and network.

The CloudLink Team is responsible for the security of the CloudLink platform software. The CloudLink platform is secured through a thorough set of practices, which include security incorporated code reviews, automated/manual testing, strict automated code/build/deploy pipeline, monitoring, and a proactive approach to ensuring software is updated and patched to mitigate against the latest vulnerabilities.

Physical Security: Infrastructure

The CloudLink platform uses Amazon for infrastructure that provides state of the art protection both at the network and physical level. AWS is responsible for physical security of the infrastructure. More details on AWS physical security are available at https://aws.amazon.com/compliance/data-center/controls. Mitel employees do not have physical access to Amazon facilities where the physical infrastructure supporting the CloudLink platform is kept.

Physical Security: Mitel Office

Visitor and access policy: physical access to Mitel corporate facilities is restricted to authorized Mitel personnel. Mitel employees do not have physical access to Amazon facilities where the physical infrastructure supporting the CloudLink platform is kept. Access to internal networks is limited to authorized and authenticated personnel only. Visitors are provided an isolated guest network access solely.