# CLOUDLINK SECURITY

VERSION 1.5

## NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

CloudLink Security
Version 1.5
August 2024

# Introduction

Applications such as Mitel One, MiTeam Meetings, Mitel Office Mobile Application (MOMA), and Mitel Office Web Application (MOWA) are Cloud-native applications. Mitel understands customer concerns when it comes to using Cloud-based solutions and therefore adopts a “continuous improvement” approach to security.  Whether it is protecting the environment our solutions operate within to conducting vulnerability testing, for example, during the research and development state, our solutions are built with security in focus. This is in alignment with the core Mitel Information Security belief that risk cannot be eliminated but can be managed.

This whitepaper presents an overview of our core communications component, “CloudLink”, used by Mitel to allow customers to seamlessly use the products and services we provide.

# CloudLink Platform

The CloudLink Platform provides unified communication, video conferencing, and recording capabilities across the multitude of applications empowered through this platform. Our solutions are subject to annual external SSAE18 Soc 2 and HIPAA Compliance audits.

Our Information Security strategy posture is aligned with the National Institute of Standards and Technology’s Cyber-Security Framework. The core standards that define the components that make up the framework is based on the internationally recognized International Standard for Information Security, ISO/IEC 27001, ISOIEC 27002.

## Physical Access

The CloudLink Platform is built on the global Amazon Web Services (AWS) Cloud. This is for two reasons:

1. With an ever-increasing global expansion business model, leveraging the capabilities of AWS facilities enables Mitel to address regional compliance concerns regarding Data location and Storage efficiently and cost effectively.

2. AWS takes data security seriously with built-in innovative security solutions and services at our disposal. Besides, the platform and data centers are subject to SSAE18SOC type 1-3 external audits twice a year, which gives us insight into the design and operational effectiveness of our data center provider.

- For a list of first class controls that AWS employs navigate to https://aws.amazon.com/compliance/resources/ and use the search tool to look for “data centers”.

## Access Control

Separation of Duties refers to the principle that no user should be given enough privileges to be able to misuse the system on their own. By default, no Mitel employee has access to production.

The system is locked and changes to production are accomplished through automation.

Access to Production is performed through a temporary access request, granting which requires proper approvals and references to the appropriate customer tickets. Least Privilege Access principles are used, so that the Mitel Employee is assigned a temporary role that limits the employee's access to a level sufficient to perform to the job at hand.

Identify Access Management (IAM) is provided through AWS's IAM services that employ AWS organizations, and Role Based Access Controls maximize the granularity of least privilege access. Multi-Factor Authentication (MFA) is used on all AWS user logins and the password rules are NIST 800-63 compliant.

Further information about AWS security can be found at these links:

- https://docs.aws.amazon.com/security/
- https://aws.amazon.com/compliance/resources/
- https://aws.amazon.com/compliance/shared-responsibility-model/

## Business Continuity and Disaster Recovery

CloudLink maintains a Business Continuity and Disaster Recovery Manual to ensure that arrangements have been made for limiting system downtime in the event of a natural or human disaster. This process is tested and reviewed annually and includes protocols that:

- Address how Mitel protects its cloud operational facilities and data against natural disasters, human error, hardware failure, and software problems
- Document plans to provide direction and control from corporate facilities during response to and recovery from disasters and to provision customer services
- Provide procedures to be followed in the restoration of environments (both internal and external) within a minimal timeframe and with minimal impact to our customers and employees
- Document the facilitation of off-site storage of backups
- Ensure that a plan for data recovery is in place.

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

## Capacity and Availability

With the infrastructure being built on top of AWS, we continuously monitor the capacity and availability of the CloudLink Platform. Alarms are triggered at various thresholds to ensure that uptime objectives are maintained.

CloudLink maintains a status page where customers can view the status of the various services provided to them. This is available at https://status.mitel.io/ .

## Change Management

CloudLink uses an integrated and automated change management process where issue tracking, source control, testing (including automated security testing), builds, and deployments are managed through a common pipeline. CloudLink supports independent development and production environments. The development and operations team in CloudLink follows a DevSecOps process that ensures that all phases of getting software to production and operating the service have security in focus. While existing static and dynamic analyses of security tools ensure that all updates and changes are protected against known threats, the inclusion of threat and risk modelling within the DevSecOps process keeps CloudLink ahead of evolving threats and potential actors.

Privacy controls are designed into the CloudLink DevSecOps process, and any new Personally Identifiable Information (PII) stored in the platform is reviewed by the Data Protection Officer's (DPO's) Office to ensure we are processing and retaining PII conforming to the requirements of legitimate use as defined by GDPR.

## Incident Management

CloudLink has a well-defined incident management process that comprises two distinct flows: one each for security-related and non-security-related incidents. While our Tier 3 support engineers will attempt to triage field found issues, there is a CloudLink Incident Response Team in place to provide expert backup to the support engineers if a situation escalates. 24/7 coverage is available for critical incidents.

CloudLink employs proactive detection of incidents via our automated service monitoring capability. Incidents that require immediate action engage the CloudLink Incident Response Team.

For security incidents, the CloudLink Incident Response Team acts as Subject Matter Experts (SMEs). There is also a corporate Security Incident Response Team (SIRT) acting as a coordinating service provider to ensure that various domains (such as Corporate Communications) are all well-coordinated, and information is reported internally and externally to Mitel in a timely fashion.

Incident status is available on CloudLink's status page at https://status.mitel.io/ .

## Services Monitoring

CloudTrail logging is enabled on the AWS-managed services that CloudLink uses (navigate to https://aws.amazon.com/compliance/resources/ and use the search tool for "aws cloudtrail faq") . This includes firewalls, proxies, and API gateways among others. In a situation in which AWS EC2 instances are involved, the syslog of the Guest OS is forwarded to AWS CloudWatch.

Log analytics is performed in Sumo Logic, where both CloudWatch and CloudTrail logs are transferred to Sumo Logic's North America instance for analysis.

## Governance

CloudLink is subject to Mitel's Global Governance policies and standards set by Mitel's Global Governance, Risk and Compliance department. This ensures that the approach to pervasive controls is aligned with internationally recognized security standards, ISO27001 and ISO27002, from both a design and an operationally effective perspective.

## Risk Management

Mitel's corporate Risk Management program is owned by the head of Mitel Legal. The risk oversight committee and custodial responsibility is jointly owned and managed by the Mitel Legal and Mitel's CISO teams. All system risks identified through external and internal audits, self-assessment through due diligence, or through incidences, are tracked in Mitel's risk registry until addressed.

## Compliances

While the AWS infrastructure that CloudLink is built on has numerous certifications and compliances, the CloudLink Platform itself is SOC2 type 1 compliant, and supports HIPAA compliance.

The CloudLink Platform performs quarterly access, firewall, and log reviews. External Penetration (PEN) testing is also performed annually.

## Encryption

Data is encrypted in transit 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 for creating a tunnel protected by 128- bit or higher Advanced Encryption Standard (AES) encryption.

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

The CloudLink Platform leverages AWS Key Management Service (KMS) and AWS-owned Customer Master Keys (CMKs) and does not currently support the import of customers' own encryption keys.

To summarize, CloudLink includes:

- Data in transit is encrypted by default using Transport Layer Security (TLS 1.2 or later) and Hypertext Transfer Protocol Secure (HTTPS) is used to provide secure endpoint communication
- Web Real-Time Communication (WebRTC) is protected by 256-bit or higher AES encryption
- Secure Real Time Protocol (SRTP) is used to secure media streams (AES 256-bit encryption)
- Data at rest is protected by AES 256-bit encryption.

## Regionalization

The CloudLink platform is deployed on AWS infrastructure within the availability zones of North America, Europe, and Asia-Pacific regions. For information about AWS regions and Availability Zones, see https://aws.amazon.com/compliance/resources/ and use the search tool for "global infrastructure".

The CloudLink platform builds on AWS' scalable, highly available, and redundant architecture of AWS. User data is retained within the home service cloud for each CloudLink account. Note that due to the dynamically elastic nature of the platform, the service may be delivered from different physical locations within an AWS Region.

Customer-generated content remains in the CloudLink region in which the customer account is registered. CloudLink generates logs for the purposes of troubleshooting, billing, maintenance, compliance, for which security and Personally Identifiable Information (PII) may be required. The analysis of the logs is performed using Sumo Logic at their North America instance.

## Customer Isolation

The CloudLink Platform follows the *pool isolation model* as defined by AWS. For more information, navigate to https://aws.amazon.com/compliance/resources/ and use the search tool to look for the term "tenant isolation".

## Data Retention

Unless your organization has otherwise agreed with Mitel, content is retained for as long as your organization has a CloudLink account and is entitled to use the CloudLink service. Event logs containing PII may be retained for a period up to seven years.

## Privacy Policy

For details of privacy policies, refer to the MiCloud Services - Global Terms of Service:

https://www.mitel.com/-/media/mitel/file/pdf/legal-docs/mnil-gtos-tmp-31jul21-v5.pdf

# Secure Applications

What makes our native CloudLink applications unique in terms of security is that we use the same DevSecOps process for the CloudLink Platform as that we use for the native CloudLink applications. The highlights of this process are:

- Development to the deployment to app store or web hosting service of the CloudLink application is through an automated CI/CD pipeline, which ensures that malicious actors cannot inject malicious code into production
- Automated security scans on each build
- External penetration testing performed on the application as part of the solution PEN test
- Employment of threat modelling as part of the development process
- Use of an automated change management process, which enforces Separation of Duties and least access privileges.

On the CL Platform, Authentication and Access for applications is managed through a native IAM system that supports OAuth 2.0 and OpenID Connect 1.0. The IAM framework also provides support for IAM federation via SAML 2.0, which allows for popular federated options such as Azure AD. The password rules are NIST 800-63 compliant by default.

Typical security controls in our applications include:

- Data in transit is encrypted by default using Transport Layer Security (TLS 1.2 or later) and Hypertext Transfer Protocol Secure (HTTPS) is used to provide secure endpoint communication
- Web Real-Time Communication (WebRTC) is protected by 256-bit or higher Advanced Encryption Standard (AES) encryption
- Secure Real Time Protocol (SRTP) is used to secure media streams (AES 256-bit encryption)
- Data at rest is protected by AES 256-bit encryption.

# Product Security Information

## Mitel Product Security Vulnerabilities

The Product Security Policy discusses how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how the reporting of security vulnerabilities is performed.

Mitel's Product Security Policy is available at:

https://www.mitel.com/support/security-advisories/mitel-product-security-policy

## Mitel Product Security Advisories

Mitel Product Security Advisories are available at:

https://www.mitel.com/support/security-advisories

## Mitel Security Documentation

Mitel security documentation includes product specific; Security Guidelines, Important Information for Customer GDPR Compliance Initiatives and Data Protection and Privacy Controls. Mitel also has Technical Papers and White papers that discuss network security and data center security.

Mitel Product Security Documentation is available at:

https://www.mitel.com/document-center

# Disclaimer

THIS SOLUTIONS ENGINEERING DOCUMENT IS PROVIDED "AS IS" AND WITHOUT WARRANTY. IN NO EVENT WILL MITEL NETWORKS CORPORATION OR ITS AFFILIATES HAVE ANY LIABILITY WHATSOEVER ARISING FROM IN CONNECTION WITH THIS DOCUMENT. You acknowledge and agree that you are solely responsible to comply with any and all laws and regulations in association with your use of CloudLink and/or other Mitel products and solutions including without limitation, laws and regulations related to call recording and data privacy. The information contained in this document is not, and should not be construed as, legal advice. Should further analysis or explanation of the subject matter be required, please contact an attorney.

Mitel
Powering connections

mitel.com