A white paper from Mitel

MICLOUD FLEX ON GOOGLE CLOUD SECURITY WHITEPAPER

Mitel
Powering connections

Google Cloud

1. Purpose

This whitepaper is intended for IT personnel, security personnel, Mitel accredited partners and Mitel personnel. Its purpose is to introduce the security aspects of the MiCloud Flex solution and the security aspects of the Google Cloud which is the environment that MiCloud Flex is deployed within. This includes the controls put in place and the products and features that are made available to customers to meet their security objectives; the policies Mitel has established, as well as options available to administrators to ensure the secure operation of the MiCloud Flex on Google Cloud solution.

2. Introduction

Mitel takes the business of security seriously by ensuring that the appropriate security measures are available for protecting the confidentiality, integrity, and availability of our customers systems and data. Mitel recognizes that security is a crucial aspect of the MiCloud Flex on Google Cloud offering and so at Mitel, the latest technologies and security best practices are used to provide a secure service.

MiCloud Flex on Google Cloud is a secure, hosted scalable Unified Communications and Collaboration (UCC) solution with a focus on high availability and dependability, allowing customers to run a wide range of Unified Communications applications.

The core telephony, collaboration and optional services operate in concert with Google Kubernetes Engine (GKE) which facilitates the use of containers. In addition, Google Compute Engine (GCE) is used to deliver Windows based applications on virtual machines. Each instance of the core services is deployed in its own container or on its own virtual machine which means that each customer's instance is isolated from all of the other customer instances via separate containers, virtual machines and their own Virtual Private Cloud (VPC) within the Google Cloud infrastructure.

A customer cannot contact another customer without routing through the Public Switched Telephone Network (PSTN), as customers are isolated from each other.

To achieve this, Mitel has created an infrastructure and architecture leveraging proven technologies onto which account administrators can layer and customize policies of their own, such as permitted user features and dialing rules.

Protecting the confidentiality, availability, and integrity of customer systems and data is of the utmost importance to Mitel. If your business has the same high standards, MiCloud Flex on Google Cloud is the ideal solution for you.

3. Overview of MiCloud Flex on Google Cloud

Unlike many other Unified Communications as a Service (UCaaS) offers which are strictly multi-tenanted solutions, MiCloud Flex solution is a hybrid solution utilizing both multi-instance and multi-tenant deployments.

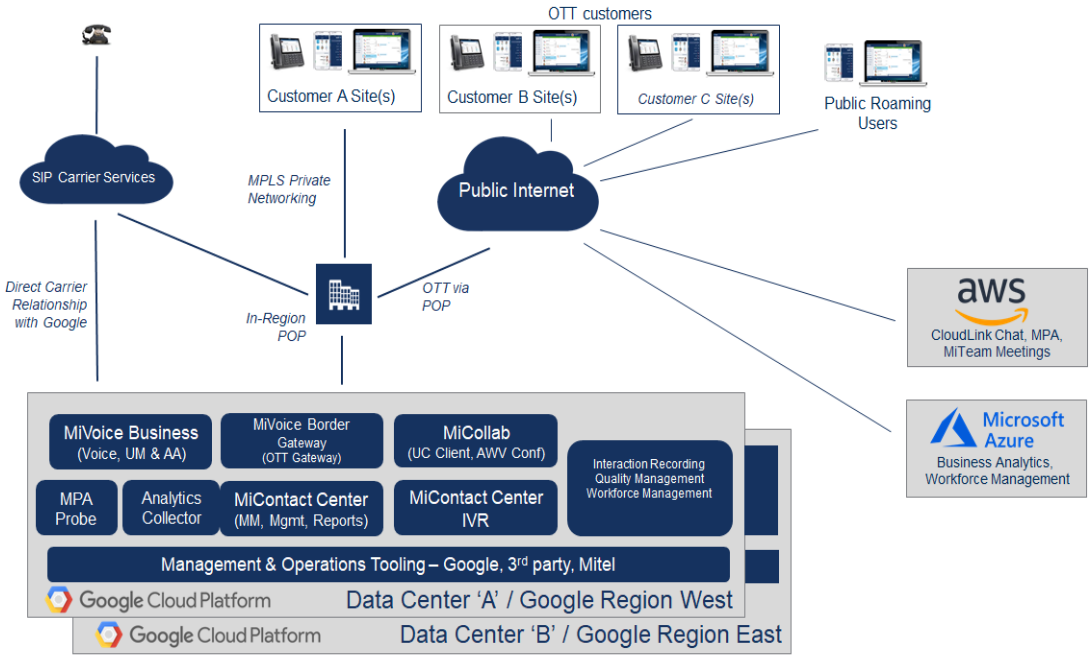
Core telephony, collaboration and key optional services are deployed as multi-instance applications in the Google Cloud environment, providing the customer with their own isolated application instances including Five "9s" availability for the core services.

Other optional services are deployed as highly available multi-tenanted solutions on Amazon Web Services (AWS) platform or on Microsoft Azure Cloud platform.

The figure below is a high-level architectural representation of MiCloud Flex on Google Cloud solution showing where the various components reside.

As can be seen in the diagram WAN connectivity, be it OTT or MPLS terminates at Mitel's regional Points of Presence (PoPs). The PoPs are in turn are uplinked securely to the Google Cloud using regional carriers with VLAN/VxC connections isolating the customer traffic.

MiCloud Flex on Google Cloud - Architecture



Core Applications – Multi-instance

The core applications, telephony, voice and collaboration tools are all deployed as multi-instance solutions within the Google Cloud infrastructure, the core components are:

1) MiVoice Business, Mitel's IP PBX / Call Control
2) MiCollab – Mitel's Unified communication and collaboration solution which includes
    a) MiCollab Audio, Web and Video (AWV) Collaboration
    b) MiCollab Presence engine with calendar integration and corporate instant messaging.
3) MiVoice Border Gateway (MiVBG), a Mitel Internet facing edge device that acts as a Session Border Controller (SBC) for SIP trunks and phones, as well as for Mitel proprietary IP phones and applications.

The application layer and derived services are all developed by Mitel, including the IP Desk phones which provides for a seamless security architecture.

All of these applications can be securely accessed by the user through the MiCollab Client – Available as a desktop client, mobile device client (Android and Apple) and through a web browser, the MiCollab Client provides access to enterprise wide instant messaging, voicemail, presence management, display and control (including calendar integration), conferencing, collaboration, and an optional softphone, all from one simple to use secure interface.

Core Applications – Multi-tenant

Mitel Performance Analytics (MPA) is a secure cloud-based management tool that is used to manage the MiCloud Flex solution. MPA is composed of two components, the management tool and a software network probe. The management tool is hosted on AWS and the network probe is hosted on Google Cloud within the MiCloud Flex deployment. MPA is deployed as a multi-tenant solution. For additional security, MPA supports two factor authentication and connects to the MiCloud Flex solution over encrypted communication channels.

To these core components, optional Mitel applications can be added.

Optional Applications – Multi-instance

The following optional applications are deployed as multi-instance solutions in the Google Cloud:

- **MiContact Center Business** – A feature rich omnichannel contact center solution
- **Mitel Workforce Optimization** suite which includes Mitel Interaction Recording, Mitel Quality Management, Mitel Speech Analytics and Mitel Workforce Management

Optional Applications – Multi-tenant

The following optional applications are deployed as multi-tenanted solutions:

- **MiTeam Meetings –** A cloud-based team instant messaging tool hosted on AWS utilized by MiCollab
- **CloudLink Chat –** A cloud-based team collaboration tool hosted on AWS utilized by MiCollab and optionally MiContact Center Business
- **Mitel Business Analytics (Tollring) –** A suite of cloud-based Business Analytics tools hosted on Azure
- **Mitel Workforce Management** powered by Teleopti/ Calabrio

Customer Access to MiCloud Flex

Access to MiCloud Flex on Google Cloud is available through MPLS service providers, which ensures a private and secured WAN service to the customer, or over the top (OTT) across the Internet.

NOTE: Not all features and services are available when connecting Over-The-Top. Refer to the MiCloud Flex Solution Engineering Guidelines.

3.1 Multi-Tenant vs. Multi-Instance

As noted in the Introduction and Overview sections, the MiCloud Flex on Google Cloud solution is based on a multi-instance architecture. There are also multi-tenant applications hosted on other cloud platforms that MiCloud Flex interfaces with.

When cloud solutions are strictly multi-tenanted, it means that a single application is tenanted so that each customer has their own space within the application, but the application is a shared resource.

Multi-tenanting allows the service provider to oversubscribe the solution, and therefore potentially reduce their own operating costs. These multi-tenanted solutions, by their definition of being tenanted, are not controlled by the customer, but by the service provider.

Additionally, with a multi-tenanted solution there is a possibility that a customer or several customers may consume resources excessively, potentially impacting not only their own ability but also other customer's ability to access resources during peak demand times.

In contrast to pure multi-tenanted solutions, MiCloud Flex core services – telephony, collaboration and key optional services - are sized to meet the customer's requirements and deployed as multi-instance solutions on the Google Cloud.

This ensures that the MiCloud Flex core services are always adequately provisioned for peak performance and that customers have direct control over their MiCloud Flex software updates.

3.2 Software Updates

With MiCloud Flex on Google Cloud, the customer has their own secure isolated instances of core applications, this means that the customer cannot have their ability to access their applications and resources impacted by other customers who might be performing their own updates.

With the exception of Google's own Google Cloud scheduled updates the customer can make their own MiCloud Flex update decisions and maintain as much control as they want. For example:

- Choose whether they want to perform an update, as the changes may or may not be applicable to their business
- Choose when to schedule the update, so that they do not disrupt their business at a critical time
- And as the core components of MiCloud Flex on Google Cloud are not a multi-tenanted solution, if one customer requires an upgrade or downtime is required to resolve a problem, other customers are not affected

This is of benefit to the customer, as MiCloud Flex on Google Cloud allows the customer to:

- Have an OpEx based managed service Cloud solution
- Still maintain as much control of their infrastructure as they want to have and
- Decide for themselves whether or not to accept updates that may or may not be relevant to their business needs

NOTE: Google makes updates for their Cloud platform software available every month. To minimize interruptions customers and partners may choose to defer the Google updates so that they align with MiCloud Flex updates, but it is recommended that Google updates are applied at least once every six months.

If Google Cloud updates are not performed on a frequent enough basis, Google will force updates, however the partner will be informed of a pending forced update via the MPA dashboard and an email message starting three months in advance of the update.

3.3 Data Backups

The partner must schedule daily full backups and weekly full backups to be performed on the customers' systems. Ensuring that backups are scheduled is the responsibility of the partner. Backups are stored in Google Cloud storage which is encrypted at rest.

NOTE: Ensuring that backups are scheduled and performed at the scheduled times is the responsibility of the partner.

4. Google Cloud – Key Features

Google Cloud is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search and YouTube. Google Cloud was built with security and availability as the primary design requirements.

The following sections summarize some of the security and availability features built into Google Cloud. For a more comprehensive description refer to the Google Cloud document called Google Security White Paper, 2019. This white paper and other Google Cloud security related information may be found at:

https://cloud.google.com/security

4.1 Google Cloud - Availability

Google Cloud data centers are designed with highly redundant components and services such as, servers, data storage networks and devices, network infrastructure, Internet connectivity and software services.

Google has geographically distributed their Google Cloud data centers on different continents and in different regions so that in the event that there is a regional disruption due to a hardware or software failure, political instability or a natural disaster, services can be switched to an alternative Google Cloud data center so that there will be no service interruption.

4.2 Google Cloud - Connectivity

Google's IP data network utilizes their own fibre networks, public fibre networks, and undersea cables. This network topology provides high availability. Due to minimal networking hops, Google's network offers very low latency on a global scale, and minimal locations in the network that could be targets for malicious actions.

When data is transmitted over a network it is vulnerable to unauthorized access, Google's networking equipment is designed and configured to ensure that the transmitted data is secured. Google only allows services and protocols that meet very strict security controls to traverse their network.

For more information refer to Google's Whitepapers; Encryption in Transit and Application Layer Transport Security, the document may be found at:

https://cloud.google.com/security

4.3 Google Cloud - Power and Environmental Controls

Google Cloud data centers are engineered to operate 24/7. To accomplish this, Google Cloud data centers utilize redundant power and environmental controls.

All critical equipment has a primary and secondary power source and backup generators can provide enough emergency electrical power to run each data center at full capacity.

Environmental systems maintain a constant operating temperature within the data center ensuring that equipment remains within its specified operating temperatures thereby reducing the risk of service outages.

Google Cloud data center Security Operations Centers and remote monitoring desks monitor the data center for unacceptable temperatures, fire and smoke.

4.4 Google Cloud - Physical Access and Employee Security Policy

4.4.1 Physical Access

Google Cloud data center physical security is based on a layered security model, which uses security personnel, electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. Google Cloud data centers are monitored 24/7 by high-resolution interior and exterior cameras with the ability to detect and track intruders. Should an incident occur, access logs, activity records, and camera footage are readily available.

Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multi-factor access control using security badges and biometrics and the actual data center floor is protected with laser beam-based intrusion detection systems.

Only approved Google employees with specific roles may enter. Less than one percent of Google employees will ever set foot in a Google Cloud data center.

4.4.2 Employee Security Policy

Prior to hiring new employees, Google will verify an individual's education and previous employment, and perform internal and external reference checks.

Where local labour law or statutory regulations permit, Google may also conduct criminal, credit, immigration, and security checks on persons applying for Google employment. The extent of these background checks is dependent on the desired position.

All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers.

4.4.3 Mitel Employee Remote Access Policy

Mitel employees do not have physical access to Google data centers. Mitel employee remote access to the MiCloud Flex Google Cloud environment is secured through the use of Google's Identity and Access Management (IAM) facilities. Google's IAM allows for the granting of granular access so that users are only granted necessary permissions to access specific resources. Remote access connectivity is via secured protocols such as TLS 1.2 or better HTTPS connections.

Mitel employs technical access controls and internal policies to prohibit employees from arbitrarily accessing user files and to restrict access to metadata and other information about users' accounts. To protect end user privacy and security, only a restricted number of operational staff responsible for developing Mitel's core services have access to the environment where user data is stored.

Access to networks is strictly limited to the minimum number of employees and services. For example, Firewall configuration is tightly controlled and limited to a small number of authorized administrators.

4.5 Google Cloud - Partner Access Policy

Mitel Partner access is provided via Mitel Performance Analytics (MPA) and is restricted to a management portal with access only to the management interfaces of the underlying applications, for user and application configuration. Partners do not have access to any of the underlying infrastructure.

Partner access to a particular customer is only available after the Mitel automated orchestration tools have instantiated and configured the underlying infrastructure, including the management portal.

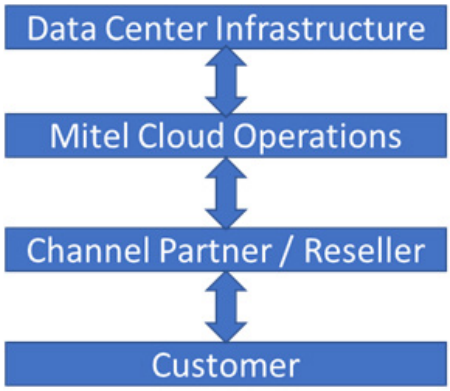
Customers have access to their own specific application portals to allow configuration of certain features and functions, including administrator password resets, and user phone-key configuration and call direction, e.g. divert to voicemail.

Users do not have access to the underlying infrastructure.

Access roles within the applications also provide user restriction access, such as allowing customer administration staff access, but restricting general users.

4.6 Compliance – A Shared Security Model

Mitel MiCloud Flex provides Unified Communications and Collaboration (UCC) services that can be configured to assist a customer with their security compliance considerations. As with any cloud-based solution the Security and Compliance needs are a shared responsibility. With MiCloud Flex the shared responsibility is between the data center providers, Mitel, the channel partner / reseller and the customer.



Data Center Infrastructure

The data center vendor(s) – in this case primarily Google are responsible for the physical security of the data center as well as the underlying infrastructure such as the host servers, containers and inter and intra zonal connectivity. The data center provider is responsible for any security patches to the underlying infrastructure including host server operating systems, container software and Kubernetes. Google Cloud security compliance is discussed in the section *Google Cloud – Security Compliance.*

The MiCloud Flex solution uses additional cloud-based platforms such as Amazon Web Services (AWS) and Microsoft Azure Cloud Services for hosting other MiCloud Flex solution components. Security compliance for these additional cloud platforms is discussed in the section *Other Cloud Based Services*.

Mitel Cloud Operations

Mitel provides the applications running the Flex service and ensures that while the applications are in an unconfigured state that a channel partner can be provided secure access to configure the service to the customer's requirements. Mitel is responsible for creating security patches for the applications.

Mitel data protection addendum and terms of service are available as follows:

- MiCloud Services – Global Terms of Service: https://www.mitel.com/en-ca/legal/mitel-cloud-services-terms-and-conditions
- Data Protection Agreement (DPA): https://www.mitel.com/en-ca/legal/gdpr/dpa
- Mitel Application Privacy Policy: https://www.mitel.com/en-ca/legal/mitel-application-privacy-policy

Channel Partner

The channel partner is responsible for the configuration and ongoing maintenance of the customer's applications (supported by Mitel as needed) and for ensuring that they are configured to the customer's stated requirements including security settings that can be configured if not already enabled by default. The channel partner is responsible for applying security patches to the applications at a time that is acceptable to the customer.

Customer

It is the responsibility of the customer to ensure that any service that they purchase meets their compliance requirements. It is also the customer's responsibility to ensure that their implementation of the solution, working with their channel partner, is compliant to the particular level or standard and that all associated data is classified appropriately for that security compliance requirement. The MiCloud Flex applications' security features and capabilities will assist customers with these needs.

4.7 Google Cloud – Security Compliance

Google Cloud products are regularly verified for security, privacy and compliance controls by third party independent organizations. Google Cloud maintains compliance certifications that are specific to certain geographic regions and also specific to industrial sectors such as government and public sector, financial services and health care.

The following is a partial list of the more common sector regulations that Google Cloud is compliant with.

Data Center

- ISO/IEC 27001/27012/27018 – Global
- SOC 1/2/3 - Global

Credit Card

- PCI DSS - Global

Healthcare

- HIPAA – US
- HDS – France
- NHS - UK

Governmental

- California Consumer Privacy Act – US
- FIPS 140-2 – US
- GDPR – Europe
- The Personal Information Protection and Electronic Documents Act – US
- UK's Cloud Security Principles - UK
- Cloud Computing Compliance Controls Catalog (C5) – Germany

For further information on Google Cloud compliance, refer to Google's compliance resource center:

https://cloud.google.com/security/compliance/

4.8 Google Cloud - Data Storage

MiCloud Flex on Google Cloud allows the customer to select the region where their content and services are hosted. After a selection is made, subject to any exceptions set out in the MiCloud Services: Global Terms of Service document, Mitel ensures that all MiCloud Flex on Google Cloud data is stored within the designated region.

The exception to the foregoing is when the customer selects multiple regions to form an international deployment. With international deployments, general user information and content is shared across all regions within the customer's dedicated environment.

A high-availability installation requires that systems are hosted in multiple regions to maintain service levels should the primary region lose service. When the primary region is selected, a designated secondary region is also defined. Systems hosted across these two regions will share configuration data to ensure that a user can obtain service from either region.

Google Cloud Data Sovereignty

The solution's core components are hosted in Google Cloud data centers:

- Americas customers access services from data centers located in the Americas, Points of Presence (PoP) are also located in the Americas
- UK customers access services from data centers located in the UK, Points of Presence (PoP) are also located in the UK
- French customers access services from a primary data center located in Belgium and a secondary data center located in the Netherlands. The Primary PoP is located in France and the secondary PoP is located in Germany.

The MiCloud Services – Global Terms of Service, supporting documents and other policy documents may be found here:

https://www.mitel.com/legal/mitel-cloud-services-terms-and-conditions

5 Other Cloud Based Services

The MiCloud Flex solution uses additional cloud-based platforms such as Amazon Web Services (AWS) and Microsoft Azure Cloud Services for providing Mitel customers with access to additional applications and services.

5.1 Amazon Web Services

Amazon Web Services (AWS) is used to host the Mitel CloudLink platform, the Mitel Performance Analytics management tool and MiTeam Meetings.

Amazon Web Services provides a highly reliable, scalable cloud infrastructure platform within the customer's geographic region. AWS services and data centers have multiple layers of operational and physical security and AWS is compliant with numerous industry-recognized security certifications and audits.

Connectivity to Amazon Web Services is via a secured channel over the Internet. For more information regarding AWS security refer to:

https://aws.amazon.com/security/

For more information regarding AWS security compliance refer to:

https://aws.amazon.com/compliance/programs/

5.1.1 Mitel CloudLink

Mitel's CloudLink platform is built on the Amazon Web Services (AWS) cloud computing platform. The AWS platform provides CloudLink users with enterprise-level high availability, stability, multi-layered security, and data protection.

The CloudLink platform is used to deliver the following applications and services.

- MiTeam Meetings - A cloud-based team collaboration tool
- CloudLink Chat - A cloud-based team collaboration tool utilized by MiCollab and optionally MiContact Center Business.
- Additional services provided by the CloudLink platform include Identity and Access Management (IAM), chat, presence, notifications, workflow, media services, and Short Message Service (SMS).

European customers will access the CloudLink services from AWS data centers located in Europe, Americas customers will access the CloudLink services from AWS data centers located in the Americas.

These applications are discussed in further detail in the section *Application Security*.

5.1.2 Mitel Performance Analytics Management Tool

Mitel Performance Analytics (MPA) is a cloud-based management tool that is hosted on AWS. MPA is the administration tool that is accessible to the Mitel partner and the customer and supports two factor authentications for secured access.

MPA is used for performing MiCloud Flex on Google Cloud system management, administration, configuration, data provisioning, voice quality monitoring, data synchronization, accounting, configuration of application interfaces and alarm and maintenance functions.

The MPA voice quality monitor can forewarn the Mitel partner of any voice quality issues, which will allow the partner to take timely corrective actions.

MPA is used with Solution Manager to manage the MiCloud Flex components, the partner will use an OTT connection to the MPA server to manage the customer.

MPA consists of two components, the MPA server and the MPA probe. The MPA server is hosted on AWS infrastructure. The MPA probe is a software application that is deployed within the MiCloud Flex network on Google Cloud.

The MPA probe communicates with the Mitel applications directly, these communications are fully contained within the network that the applications and probe are deployed within on the Google Cloud. The MPA probe connects to the MPA server over the Internet.

The MPA probe forwards status and events from the MiCloud Flex network and provides a web portal with access security to native management interfaces.

The MPA probe performs some caching of status and events in the event of communication difficulties between the probe and the MPA server.

MPA in conjunction with the probe supports a Remote Access Service to MiContact Center Business and to Mitel Interaction Recording.

MPA Remote Access provides a number of key advantages:

- There is generally no need to configure firewall rules at either end of the remote connection because MPA Remote Access uses outbound connections from the Probe employing standard TCP/IP protocols.
- No VPN server or client software is required, at either end of the remote connection.
- The MPA Remote Access service manages all of the security tokens required to establish a secure remote connection, avoiding the need to maintain multiple lists of VPN access credentials.

The MPA communication links are secured using industry standard encryption and authentication mechanisms.

- System Authentication: MPA uses a 2048-bit security certificate and authenticates all connection requests.
- TLS: All TLS sessions to MPA are encrypted and authenticated using RSA-2048 for key exchange and AES 128 for encryption.

- SSH: All SSH sessions are encrypted and authenticated using RSA-1024 with a rotation for key exchange and AES 128 for encryption. Key Rotation is enabled and generates a new key for each session.

For more information on MPA security refer to the document Mitel Performance Analytics, found at:

https://www.mitel.com/en-ca/document-center/security/technical-papers

5.2 Microsoft Azure Cloud Services

MiCloud Flex on Google Cloud customers are able to access Business Analytics and Workforce Management applications that are hosted on Microsoft Azure Cloud Services platform.

The Business Analytics and Workforce Management applications that are available, work in conjunction with Mitel's Unified Communications applications which gives customers the ability to optimize their business operations.

Connectivity to the Azure platform from the customer's site is via a secured channel over the Internet. The Azure platform is designed with multi-layered security controls which are applied to Azure data centers, infrastructure and operations. Azure is deployed in globally distributed data centers providing geographic resiliency and reliability.

Azure is compliant with numerous industry-recognized security certifications and audits.

For more information related to Microsoft Azure Cloud Services, refer to:

https://azure.microsoft.com/en-ca/overview/#security

5.2.1 MiCloud Business Analytics - Tollring

Tollring is the provider of Mitel's cloud-based Business Analytics. MiCloud Flex on Google Cloud employs Tollring's Insight and Report Licensed Capabilities products.

Tollring applications are hosted on Microsoft Azure Cloud platform, and there are numerous Azure Cloud data centers that are globally distributed. The location of the Azure Cloud data center will be determined by where the customer is located and the customer's own requirements.

European customers will use the Azure data center in the Netherlands, there are also Azure data centers located in the U.S., the UK and Australia.

Tollring applications collect SMDR data from the MiVB, the data collected is then processed by Tollring to create online dashboards and reports detailing business communications usage and call statistics on a per user basis.

Access to Tollring technology resources is only permitted through secure connectivity (VPN) and requires authentication. Tollring's password policy requires complexity, expiration and lockout.

Access to resources is restricted and closely monitored. Access is granted only for the period necessary to perform administrative or technical support tasks and is revoked after tasks are completed. All permissions are reviewed quarterly.

Tollring ensures that all data transmissions are encrypted using secure TLS cryptographic protocols and that data at rest is also encrypted.

Tollring is compliant with the ISO 27001 Information Security Standard and ISO 9001 Quality Management System. Tollring re-certifies those compliances annually. Tollring is compliant with and follows the General Data Protection Regulation (GDPR).

Further information about Tollring's company policies, security compliances, security practices and white papers may be found at:

https://tollring.com/policies

5.2.2 Mitel Workforce Management

An important component of Mitel's Workforce Optimization (WFO) suite is Mitel Workforce Management (WFM) powered by Teleopti/Calabrio. Mitel's WFM solution integrates with MiContact Center Business and provides MiCloud Flex on Google Cloud customers with an enterprise caliber workforce management solution.

Mitel Workforce Management is hosted on Microsoft Azure Cloud platform which ensures a high level of availability. Customers are able to select AWS data centers in a geographic region that is appropriate for their requirements.

Mitel Workforce Management software and applications encrypt all customer data, while in use, transit and while at rest.

Teleopti/Calabrio has experience and knowledge related to helping customers understand how to meet the requirements of PCI, HIPAA, Sarbanes-Oxley, Frank-Dodd, or MiFID. Calabrio can provide contact center managers with tools to detect fraud, conduct investigations and mitigate specific security risks in a wide range of markets, including financial, retail, government and healthcare.

Teleopti/Calabrio has published a number of security documents that discuss PCI requirements, GDPR requirements, CCPA requirements and Cloud security, these documents are located at the following sites.

https://www.calabrio.com/resource-center/white-papers-reports/

https://www.calabrio.com/resource-center/collateral/

For further information related to achieving security compliances within the contact center, refer to:

https://www.calabrio.com/contact-center-compliance/

6. Network Security and Connectivity

Mitel diligently maintains the security of the back-end network. Mitel identifies and mitigates risks via regular application, network, and other security testing and auditing by both internal security teams and third-party security specialists.

Mitel's network security and monitoring techniques are designed to provide multiple layers of protection and defense-in-depth strategies.

Mitel employs industry-standard protection techniques, including firewalls, network security monitoring, and customer ingress and egress intrusion detection systems to ensure only eligible traffic can reach Google Cloud infrastructure.

6.1 Point of Presence

A Point of Presence (PoP) is a local access point, All Mitel PoPs are located in Tier3+ data center facilities. The PoP interconnects the customer's network or a user's Teleworker device to the MiCloud Flex on Google Cloud solution.

Connections from the customer site to the PoP can be made via an MPLS connection or an Over-The-Top connection (OTT). SIP Carrier services that have been approved by the Mitel Solution Alliance team (MSA).) are also terminated in the PoP.

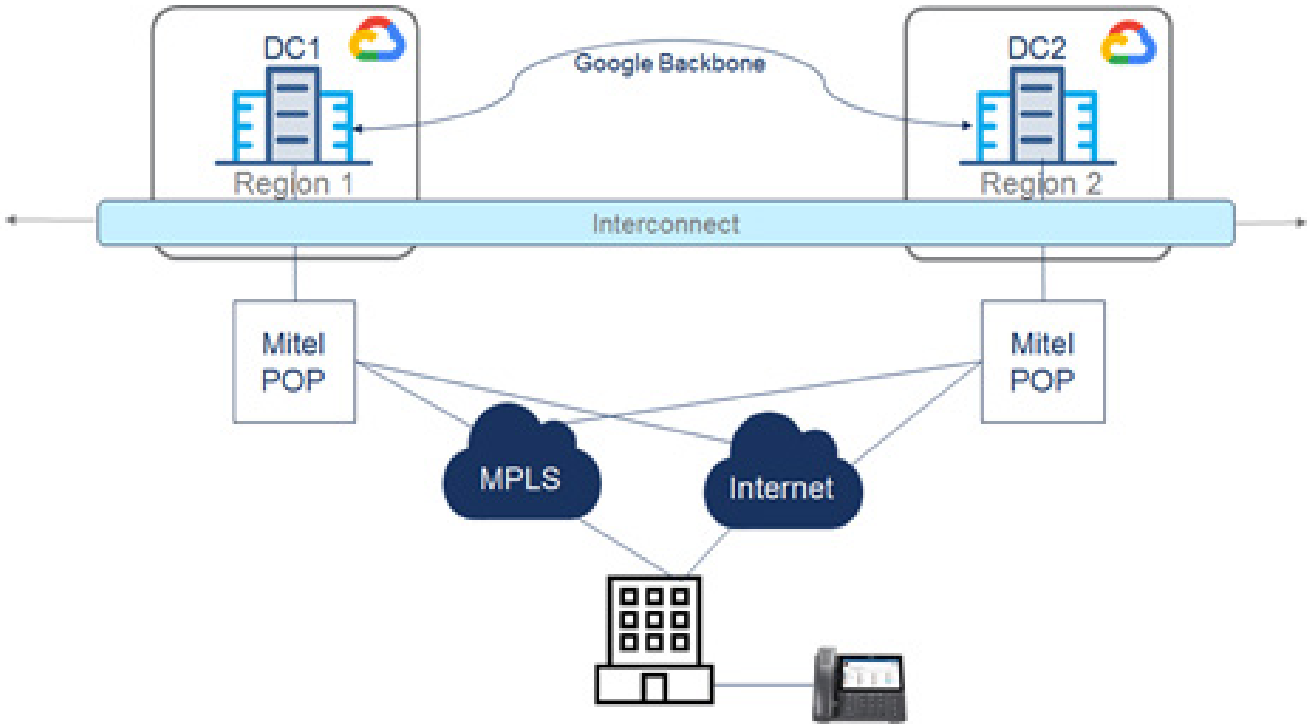
Connectivity between most North American PoP locations and the MiCloud Flex on Google Cloud data center is accomplished via Megaport's Software Defined Network (SDN) and their Megaport Cloud Routers (MCR). In Europe alternate SDN WAN providers may be used to provide connectivity between the PoP and the MiCloud Flex on Google Cloud data center.

The Megaport connections are logically divided into different VLANS and Virtual Cross Connect (VxC) configurations to create dedicated VPC/VLANs.

When a customer is connecting to the PoP with an MPLS WAN or an MPLS WAN and an OTT connection the VxC for this customer will all traffic for that specific customer between the PoP and the Google Cloud.

For customers that choose to only use OTT connections to the PoP, a single VxC connection can be shared by multiple OTT-only customers.

NOTE: Some regions may not use Megaport's SDN, alternative SDN providers are Colt and Equinix.



Mitel operates PoP locations which are located in geographically different regions and PoPs in different geographic regions are grouped together into pairs. The paired PoPs operate in a redundant configuration which means that if there is a fault at one PoP, or a connectivity failure associated with one PoP, the other PoP will continue to provide the customer with connectivity to MiCloud Flex on Google Cloud.

The redundant PoP configuration is key to providing customers with Five '9s' of availability for connections to the Google Cloud.

For details on where Mitel PoPs are located refer to the Mitel document, MiCloud Flex Solution Engineering Guidelines, which may be found at https://www.mitel.com/.

6.2 OTT Connectivity

Traffic originating from devices connected via the Internet such as OTT users and Teleworkers first connects to a Mitel PoP. Access into the PoP is controlled by a redundant firewall in each PoP and once the traffic has been validated, the PoP then forwards the traffic to the Cloud router which connects to the Google Cloud over a Virtual Private Circuit (VPC).

Before the traffic is granted access to the Google Cloud, the traffic must be further authenticated by the MiVoice Border Gateway, a Session Border Controller that is designed for Mitel solutions.

6.3 MPLS Connectivity

When using a private MPLS WAN to connect the customer site to the PoP, the PoP will forward the traffic to the cloud router which ensures that only valid traffic is passed onto the customer's dedicated VPC. Mitel devices further protect the traffic by encrypting signaling with TLS 1.2 and audio and video with SRTP 128-bit AES encryption.

6.4 Mixed Connectivity

MiCloud Flex on Google Cloud supports mixed connectivity, meaning that connections may be made over an MPLS connection and also an Over-The-Top Internet (OTT) connection so that users located at the customer's site and also remote workers can be connected simultaneously, however a user cannot be both an OTT user and an MPLS user from the same desktop.

6.5 SIP Trunk Connectivity

SIP Trunks provided through the channel partner are connected via the PoP over the Internet or over a dedicated carrier link using a publicly routable IP address.

The SIP Trunk traffic is further authenticated by the MiVoice Border Gateway, a Mitel purpose-built Session Border Controller which supports SIP signaling encryption using TLS 1.2 and Secure Real Time Protocol (SRTP).

NOTE: To ensure the security of SIP trunk traffic the SIP Carrier must also support TLS 1.2 and SRTP.

6.6 Customer Isolation

As noted elsewhere is this document, the core telephony and collaboration applications and key optional services are deployed as multi-instance applications in the Google Cloud environment.

Each customer's applications are installed in the customer's own dedicated containers (Linux based) or on dedicated virtual machines (Windows based) within Google Cloud, customers are isolated from each other and traffic cannot pass between different customers within the Google Cloud.

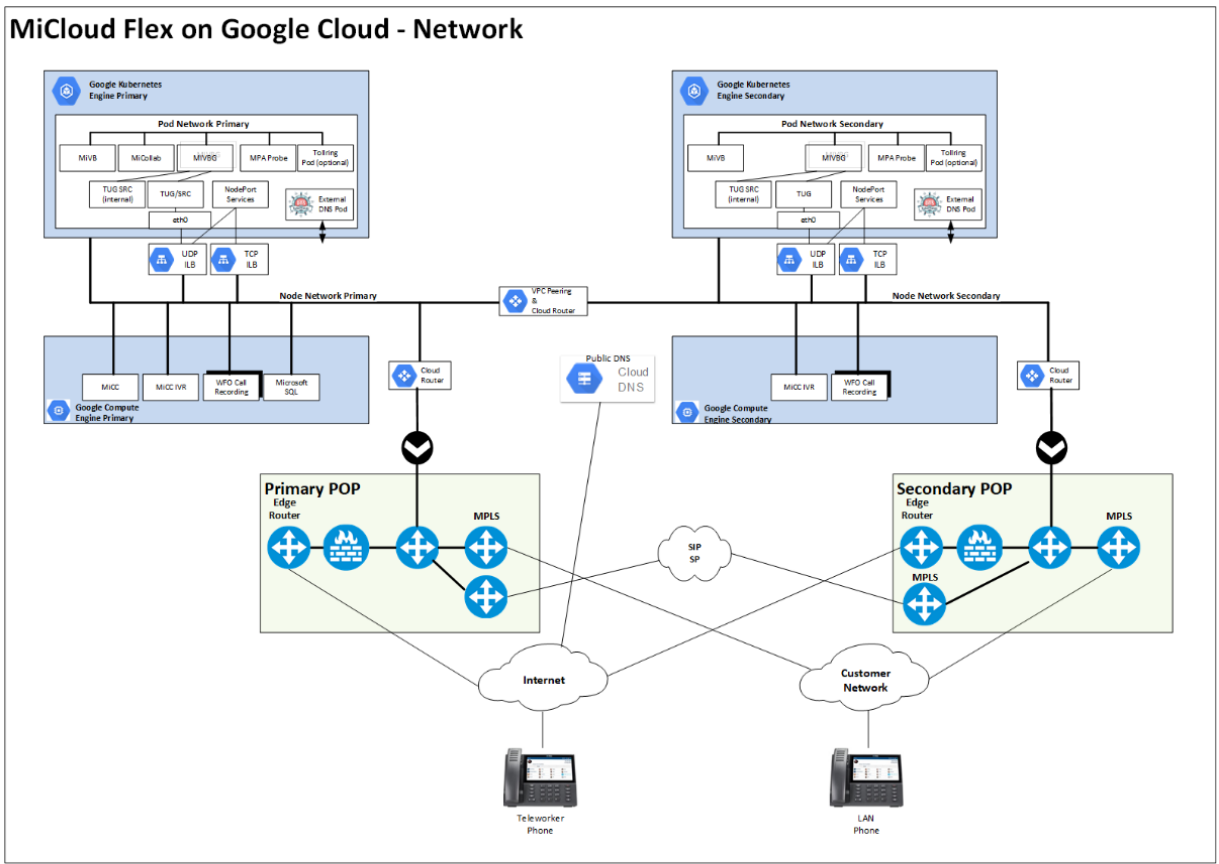
Customer isolation is an important security feature of MiCloud Flex on Google Cloud. The customer's data is isolated from other customer's data from the entry into the PoP through to the individual networks and compute engines.

Customers are separated from each other through the use of different VLANs and also Virtual Cross Connect (VxC) configurations across the interconnect between the PoP and the Google Cloud..

When a customer is utilizing both an OTT and an MPLS WAN to connect users to the PoP, the VxC for this customer will carry both OTT and MPLS traffic for that specific customer between the PoP and the Google Cloud.

For customers that choose to only use OTT connections to the PoP, a single VxC connection can be shared by multiple OTT-only customers. With this configuration customer isolation is achieved through the use of the public IP addresses and firewall rules.

The following diagram depicts the MiCloud Flex on Google Cloud network topology.



6.7 PoP Facilities - Physical Access and Employee Policy

6.7.1 Physical Access

Physical access to the PoP facilities where networking equipment resides is restricted to only personnel authorized by Mitel, as required to perform their job function.

There must be a very good reason for an individual to visit the PoP facility since most work can be carried out via a Remote Hands request.

Should there be a need for authorized personnel to visit the facility, a ticketing system is used to arrange the visit. A record of the access request, justification, and approval are recorded by management, and access is granted by appropriate individuals. An audit record of all changes made by the individual during the access is logged. Once approval is received, a responsible member of the Infrastructure Team contacts the appropriate subservice organization to request access for the approved individual.

The individual visiting the facility needs to book access in advance and may be subject to screening to confirm identification. This may include biometric data as well as authentication paperwork and then they will be signed in through security.

6.7.2 Employee Policy

Mitel employee hiring and on-boarding require background checks, security policy acknowledgement, communicating updates to security policy, and non-disclosure agreements.

All Mitel employees are also required to pass an annual code of conduct training course that includes data privacy and security.

Mitel employee off-boarding procedures ensure that all access to facilities and services are revoked immediately.

7. Application Security

The primary security concerns for IP Telephony, UC applications and networks can be summarized as follows:

- **Confidentiality:** The need to protect transmissions, whether for voice-streaming, video streaming or data services, to prevent eavesdropping or interception of conversations, conferences, call control signaling or passwords and the confidentiality of data storage.
- **Integrity:** The need to ensure that information is not modified by unauthorized users and to unequivocally prove a user or application is authorized to perform the task / function they are requesting, be it a voice call, video conference or a configuration change.
- **Availability:** The need to ensure the operation of the solution at all times.

7.1 Mitel IP Phones with MiCloud Flex on Google Cloud

The following phones are supported with MiCloud Flex on Google Cloud:

- 6905
- 6910
- 6920
- 6930
- 6940
- 6970
- MiVoice Business Console
- Wireless and DECT Phones
- RFP 12, 44, 45, 47, 48
- 112 DECT
- 612d, 622d and 623d
- MiCollab Softphones including:
- UC Endpoint SIP Softphone, and
- ACD Hot Desking SIP Softphone

7.1.1 Mitel Authentication: Known Devices and Users Only

With MiCloud Flex on Google Cloud, all IP Telephony devices and applications are reliant on the hosted call control engine for call establishment, tear down, transfer, etc. The MiCloud Flex on Google Cloud call control engine must authenticate the device or application prior to providing it with service.

Mitel phone authentication requires a unique association of device MAC addresses, Mitel set type and user-entered PIN registration numbers to successfully register with the call control engine. All communications are sent and received across a TLS encrypted channel.

Additionally, desktop phone software downloads are cryptographically protected.

SIP devices require a username and password combination. Mitel forces the use of strong username / password combinations which are sent and received across a TLS encrypted channel.

For sites where customers have controlled the access to their LANs with the IEEE 802.1X authentication protocol, Mitel also provides the option for IP phones to use 802.1X authentication.

Current models of Mitel IP phones support the IEEE 802.1X authentication protocol. Most phones support EAP-MD5, EAP-PEAP, and proxy logoff. The 6905, 6910, 6920, 6930, 6940 and 6970 also support EAP-TLS.

7.1.2 Call Signaling

To be able to make a call, a device must be authenticated and registered with the call control engine as described above.

Assuming the device has registered successfully, the call control engine then determines if a device is authorized to use a feature based on the device's Class of Service (CoS) or make a given call based upon its dialing privileges Class of Restriction (CoR).

This authentication decision to allow or bar a call or use a feature is invoked each time a user uses their device.

Signaling between MiCloud Flex on Google Cloud and a Mitel IP phone uses a proprietary signaling protocol known as MiNET which is sent and received over a Transport Layer Security (TLS) encrypted channel. Secure MiNET is the default encryption method

MiCloud Flex on Google Cloud also supports Mitel softphones which are SIP based, and Mitel approved standards-based SIP devices, all communications between the SIP device and MiCloud Flex on Google Cloud are sent and received over a SIP TLS encrypted channel.

MiNET and SIP call signaling protocols are supported simultaneously from the same system.

7.1.3 The Media Path

With MiCloud Flex on Google Cloud, the encrypted voice and video IP media packets are routed over the optimum network path. That is packets do not 'hairpin' through the data center unnecessarily. This results in reduced WAN bandwidth requirements and call latency is optimized and this results in improved call quality.

The MiCloud Flex call control engine simply provides the devices with the details needed to establish a direct media path between one another and the media then takes the optimal path.

By default, with Mitel IP phones the media path encryption is accomplished with Secure Real Time Transport Protocol (SRTP) using 128-bit Advanced Encryption Standard (AES).

SRTP requires consistent end-to-end encrypted media negotiations; therefore, every component that negotiates SRTP with a SIP endpoint must comply with RFC 4568.

7.2 MiCollab Client

The MiCollab Client application allows a user to securely collaborate with other users from their desktop. It gives users full access to their Mitel accounts and runs on Windows or Mac operating systems with presence management, unified messaging access, video chat, instant messaging, collaboration and an optional softphone and is also available through web browser access. It allows users to access functionality through their browser across HTTPS / TLS connections without installing a client.

The desktop client application is distributed by the administrator and users cannot connect without the express consent of the administrator.

Communications between the client and the MiCollab server are across HTTPS connections with Transport Layer Security (TLS) 1.2.

The same MiCollab user functionality is also available from a mobile device with the Mitel app available for iOS, Android, mobile devices, and tablets, allowing users to collaborate while on the go. Communications are across HTTPS connections with Transport Layer Security (TLS).

MiCollab Mobile Clients are distributed through the Google Play store and the Apple Store.

The optional softphone available for the desktop or mobile MiCollab clients has an encrypted call path (SRTP) and an encrypted call signaling path (SIP TLS). Non-voice communications continue to use HTTPS / TLS. The desktop softphone is often used in combination with the MiContact Center Business application so that agents do not require a desk phone.

For MPLS connected systems, MiCollab client users authenticate with the MiCollab server typically via Active Directory integration (recommended) for single sign on, though local authentication is also supported, so that password and other security rules governed by the AD administrator can be utilized. AD authentication requires that a private WAN connection is used to connected to the customer AD server. AD integration is not supported when using OTT connections.

For MiCollab connections, both internal (MPLS) and external connections, the Let's Encrypt certificate is used. The internal connections require the use of split DNS to ensure that the FQDN in the certificate is used by both internal and external connections.

7.2.1 MiTeam Meetings and CloudLink Chat

MiTeam Meetings

MiTeam Meetings is a CloudLink based multi-party video solution designed for MiCollab users who want to improve work efficiency and enhance workplace communication with seamless transitions between voice, video, and chat capabilities for a complete collaboration experience. It enables users to access features such as:

- Collaborate: Perform audio, video, and web sharing
- Chat: Hold chat sessions and receive chat notifications within a meeting
- File Sharing: Store and share files

The MiTeam Meetings service is hosted on the Amazon Web Services (AWS) cloud computing platform using Amazon's Simple Storage Service (S3).

CloudLink Chat

CloudLink Chat is a Chat application that is enabled by the CloudLink Platform. Files and links in CloudLink Chat are not executed by the CloudLink Chat service and the Chat service does not access any content uploaded by the user. It is recommended that the customer install the appropriate antivirus and malware software on their device.

CloudLink Chat runs on a serverless deployment using Amazon Web Services (AWS) S3 ElasticSearch foundation services to store data.

Data in Transit

Data in transit between a Mitel client (desktop, mobile, API, or web) and the hosted service is always encrypted via TLS 1.2 and Web Real-Time Communications (WebRTC) is protected by 256-bit or higher Advanced Encryption Standard (AES) encryption. Mitel uses strong ciphers and supports perfect forward secrecy. Individual sessions are identified and re-verified with each transaction, using a unique token created at login.

Data at Rest

Server-Side Encryption (SSE) is used to encrypt the data stored at rest in Amazon S3. Amazon S3 Server-Side Encryption employs strong multi-factor encryption. Each object is encrypted with a unique key. As an additional safeguard, this key itself is encrypted with a regularly rotated master key.

Security documentation for MiTeam Meetings and CloudLink Chat may be found at:

https://www.mitel.com/en-ca/document-center/security

7.3 MiContact Center Business

For MPLS connected systems, contact center agents use the browser accessed Mitel Ignite client for their contact center agent experience. Agents can authenticate with the MiContact Center Business server via Active Directory integration for single sign on (recommended) or through local authentication. Browser access uses HTTPS/TLS for communication between the agent's Ignite web client and the MiContact Center Business server.

This functionality is available to OTT and MPLS connected customers, with the exception of AD integration which requires MPLS connectivity.

7.3.1 Workforce Optimization - Mitel Interaction Recording (Call and screen recording)

Mitel offers advanced capabilities that can be leveraged by Cloud deployments that fall within the "Mitel Workforce Optimization" suite. As part of Mitel's Workforce Optimization (WFO) suite, Mitel has four applications that come from Mitel's OEM partner, ASC Technologies, including:

- Mitel Interaction Recording (Call and Screen Recording)
- Mitel Quality Management (Quality Management)
- Mitel Coaching and Learning (included in the Quality Management module)
- Mitel Speech Analytics (Transcription and Keyword spotting)

This release of MiCloud Flex on Google Cloud provides the Mitel Interaction Recording solution as an option. Mitel Interaction Recording is the base to offer Mitel Quality Management, Mitel Speech Analytics and Mitel Coaching and Learning. Quality Management is required to offer Speech Analytics.

Mitel Interaction Recording and analytics products are in compliance with the highest security requirements and regulations such as MiFID II.

Mitel Interaction Recording is hosted on the Google Cloud. This allows for a high level of service availability and provides customers with the ability to choose a Google Cloud datacenter in a geographic region that meets their requirements.

Customers in sectors such as emergency services and financial services need to ensure that transactional recordings will be completely intact and permanent even in the event of a system failure. Mitel Interaction Recording's high level of availability ensures that these regulatory requirements pertaining to recording system availability can be met.

The recording and storage of customer transactions and conversations must be performed with the highest security protections in order to prevent access by unauthorized personnel.

Data encryption is a mandatory requirement. As such, data in transit is encrypted and the application is capable of recording all conversations in encrypted formats.

All system user and administrative activity and interactions are monitored and logged in detailed audit logs. These audit logs are kept, providing the customer with a full audit trail.

Documentation for Mitel Interaction Recording is available on Mitel's Document Center.

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

ASC Technologies' web site is located at:

https://asctechnologies.com/english/index.html

ASC Technologies compliance information related to fraud detection, MiFID II, FinVermV and GDPR can be found at the following location:

https://asctechnologies.com/english/compliance.html

7.4 Teleworker Capability

All of the Mitel IP phones and a number of the applications offered by the MiCloud Flex on Google Cloud solution are available to be connected to the Google Cloud over the Internet securely using the MiVoice Border Gateway (MiVBG) as the Internet facing Mitel application proxy and Session Border Controller.

For details on which applications are available, refer to the MiCloud Flex on Google Cloud Engineering Guidelines.

This is also known as the Mitel Teleworker Service which securely connects remote IP phones, softphones and Mitel applications, such as collaboration and contact center tools to the data center providing full access to Mitel services all without the need for a VPN.

Voice communications are authenticated before being allowed access through the MiVBG where they are then further authenticated against the actual application.

UDP ports are opened and closed on call set up and tear down so that ports are not open without a valid call. Voice signaling is encrypted with TLS and media streams with SRTP.

Teleworker security is discussed further in the Mitel document Security and the Teleworker Whitepaper, which can be found at:

https://www.mitel.com/en-ca/document-center/security/technical-papers

8 MiCloud Flex on Google Cloud - Availability

A communication and collaboration system must be reliable, and a key feature of MiCloud Flex on Google Cloud solution is its availability.

To that end, Mitel has developed the MiCloud Flex Google Cloud solution with multiple layers of redundancy and resiliency to guard against data loss and ensure availability.

To enhance service availability Google data centers are distributed globally into different regions and countries. In geographically large countries Google may sub-divide the country into separate regions.

Google refers to a data center deployment location as a zone, a zone usually has just one data center although some zones may have more than one data center.

Regions contain multiple data centers or zones, typically there are at least 3 zones per region.

Google's data center distribution model provides users that access Google based services from within just one region with a high level of availability.

However, there is a possibility that all the zones within a region may be impacted by a common incident, for example weather conditions, floods, earthquake, etc.

In order to improve the availability of the core services available with MiCloud Flex, and to counter the threat of a large incident in one region impacting service availability, the MiCloud Flex solution is deployed in two different regions. A primary data center is located in one region and a secondary data center is located in a geographically different region.

Deploying MiCloud Flex in two geographically different regions ensures that a system is always available, even if one of the regions becomes unavailable.

Google provides connectivity on their data backbone between data centers in different regions.

Connections within a region can be considered as Layer 2 connections, as they can share a common subnet. Connections between regions are considered as Layer 3 connections, being in different subnets, and as a result require the intervention of the Google Cloud Router.

When installed in dual data centers, several of the Mitel applications, including IP telephony, have built in application level resiliency whereby the applications (or end points) switch to the secondary data center in the event of a problem being detected.

Five '9's Availability for Core Applications

Deployment across different regions offers Five '9s' (99.999%) of service availability. This availability is offered across the core voice services. It does not apply to all of the applications.

The core voice services that are offered with Five '9s' of availability are:

- MiVoice Business - Call Control
- MiVoice Border Gateway – SBC Function
- Mitel Performance Analytics – Management
- MiContact Center IVR – Contact Center
- Mitel Interaction Recording
- MiCollab Softphone – Calling Functionality
- Mitel IP Phones, MiNET and SIP
- Mitel approved 3rd Party SIP Phones

Availability of Non-core Applications

The availability of non-core applications varies based on how the application is designed and also how the application is deployed. Resilient operation of non-core applications is identified in the following table.

Application	Primary	Secondary	Resilient	Primary Service outage outcomes
MiVoice Business Call Control	Yes	Yes	Yes	Voice Service switches to secondary controller
MiVoice Border Gateway	Yes	Yes	Yes	Voice Service switches to secondary gateway
MPA Management	Yes	Yes	Yes	Dual deployment allows access to both primary and secondary regions
MiContact Center Business	Yes			Available on recovery of primary service
MiContact Center IVR	Yes	Yes	Yes	Voice Services and call routing continue in service. The SIP SP must also be configured to route to both primary and secondary gateways
Call Recording & Playback	Yes		Yes	Call playback and access to the database will not be available. Available on recovery of primary service
Call Recorders	Yes	Yes	Yes	Call recording of voice, and CTI connections (call status), continue in service. Recordings are cached until the core storage and playback server returns to service, then data is uploaded for future storage and playback access
Screen Recorders	Yes			Screen recordings are available on recovery of primary service
MiCollab Softphone Call	Yes	Yes	Yes	Softphone will re-home to primary or secondary region. Calls can be made and received.
MiCollab Softphone Directory Calling	Yes			Directory lookup may be impaired for new searches. Cached information may still be used.
MiCollab Chat	Yes		Yes	MiCollab Chat redirects to use the CloudLink Chat on AWS. Once connection is established, connection is direct to CloudLink chat.
MiCollab Presence	Yes			MiCollab Presence information will become available on recovery of the primary service.
MiCollab AWV Collaboration	Yes			MiCollab Collaboration will become available on recovery of the primary service. MiCollab Collaboration using MiTeam and CloudLink will continue to be available
MiTeam Meetings	Yes		Yes	MiTeam meetings are provided via CloudLink MiTeam Meetings application. MiCollab is used primarily for management and initial configuration.
MiNET Phones	Yes	Yes	Yes	Service moves to secondary gateway or controller
3rd party SIP phones	Yes	Yes	Yes	For phones that support DNS-SRV, service switches to secondary gateway or controller

9. Management Features

MiCloud Flex on Google Cloud is designed with multiple layers of protection, covering data transfer, encryption, network configuration, and application-level controls, all distributed across a scalable, global, and secure infrastructure.

MiCloud Flex on Google Cloud authorized users can access their data through robust access controls defined at deployment. With the MiCloud Flex on Google Cloud multi-instance architecture delivering the service, customers are assured that information is not shared and is isolated to their environment, enhancing security.

9.1 Management Access Control

Mitel applications offer capabilities to define, enforce, and manage user access policies across MiCloud Flex on Google Cloud service. These include:

- Audit trails track application changes logging the date, time, changes made, and the user that performed the modification.
- Integration with the customers Active Directory or LDAP compliant identity broker for user authentication and provisioning is supported with MPLS connected systems.
- Password policies that force users to use strong passwords. Such policies can include:
    - Password length and formation

9.2 Password Control

MiCloud Flex on Google Cloud enforces password policies. Administrative accounts must be configured to comply with the following password constraints:

- Require at least one of each the following character elements:
    - Lower-case letter
    - Upper-case letter
    - Numeric Digit
    - 'Special' character enforcement, e.g. !@££()*&^%$;:'\|"[]{}=+-_<>/?`~

10. Toll Fraud Management

Toll fraud is the action of an unauthorized use of a business' telephone system and carrier services. The primary purposes for this are to profit from a toll line and international revenue sharing fraud.

Mitel implements several controls to restrict user feature access and dialing rules. These include:

- Class of Service
- Class of Restriction
- Interconnect Restrict
- Account codes

These controls are used to define the available features, dialing restrictions, and interconnectivity of devices and trunks in predefined situations.

It is the partner's and/or the customer's responsibility to ensure that the feature access and dialing rules are correctly configured to protect the customer from toll fraud. Mitel can only provide recommendations.

Ensuring that dialing rules and restrictions on SIP trunks provided by SIP trunk providers are correctly configured is the responsibility of the partner.

10.1 International Dialing Restrictions

The default configuration for customers can be templated to deny access to dial all or specific international and premium rate numbers. Mitel recommends that calls to pay-per-call and pay-per-minute services (potentially including directory assistance services) are templated, so they are blocked by default. Ensuring that dialing restrictions and ARS are correctly configured is the responsibility of the partner.

11. Data Privacy

Guarding users' privacy and that of their business data is taken seriously at Mitel. Mitel works hard to protect user information from unauthorized access.

All data requests are scrutinized to make sure they comply with the law and Mitel is committed to giving users notice, as permitted by law when their accounts are identified in a law enforcement request.

Only data required to provide the UCC services is collected and processed.

11.1 GDPR

Respecting the privacy of our customers and partners has always been integral to the way Mitel operates.

As a data processor, Mitel provides a pre-signed Data Processing Addendum (DPA), which outlines how we process customer data when we provide MiCloud Flex on Google Cloud services. Mitel's DPA meets the requirements of GDPR Article 28.

https://www.mitel.com/legal/gdpr/dpa

11.2 Product Security Documentation

GDPR documentation for individual Mitel products and applications that are included in the MiCloud Flex solution can be found at:

https://www.mitel.com/en-ca/document-center/security/personal-data-protection-and-privacy-controls

Other MiCloud Flex security documentation can be found at

https://www.mitel.com/en-ca/document-center/security/technical-papersxt

12. Summary

MiCloud Flex on Google Cloud offers easy-to-use tools to help deliver enterprise class unified communications to its customers, without sacrificing the security that organizations require.

With a multi-layered approach that combines a robust back-end infrastructure with a customizable set of policies, we provide businesses a powerful solution that can be tailored to their unique needs.

To learn more about MiCloud Flex on Google Cloud, contact Mitel or one of our approved partners at:

- Mitel: http://www.mitel.com/contact-mitel
- Partners: http://www.mitel.com/partners

13. Need to Know More?

Mitel has several whitepapers available that offer detailed descriptions of the security measures in place at Mitel.

Name	Description	Link
Mitel Secure Development Life Cycle	This paper provides an overview Mitel's Secure Development Life Cycle (MiSDLC), the customer benefits and the key aspects of MiSDLC. This paper also covers the key components of Mitel's Product Security Incident Response Process (PSIRT).	https://www.mitel.com/en-ca/document-center/security
Mitel's Product Security Policy	The Product Security Policy discusses how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how the reporting of security vulnerabilities is performed.	https://www.mitel.com/support/security-advisories/mitel-product-security-policy
Mitel Product Security Advisories	Product Security Advisories are published for moderate and high-risk security issues.	https://www.mitel.com/support/security-advisories

To find out more about MiCloud Flex Please visit:
www.mitel.com/products/business-phone-systems/cloud/micloud-flex