Unify Phone

Data Security and Privacy; Cloud security model

Security and Privacy Unify Phone
26-10-2023

Rob Keenan, Product Manager Unify Phone

Unify® | NOW PART OF Mitel®

Unify Phone

The best of all worlds with hybrid cloud

Cloud

Unify Video by RingCentral

Voice Experience

Collaboration

Frontline Workers

SDK

Customize

Integrates with cloud applications for collaboration or mission-critical communications.

Hybrid

Unify Phone

Unify Phone offers a unified experience for telephony on any device.

On-Premises

OpenScape Business

OpenScape 4000

OpenScape Voice

MiVoice Business
MX-One
MiVoice 5000

Through connection to OpenScape/Mitel platforms.

Unify | NOW PART OF Mitel

Unify Phone

One solution – multiple user deployment options

Unify Phone for Unify Video

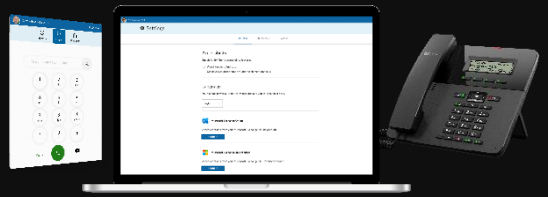
Available Now

Unify Video by RingCentral

Customers needing cloud-based messaging and meetings but appreciating the control OpenScape telephony brings blended with a great user experience.

Unify Phone for OpenScape

Available Now

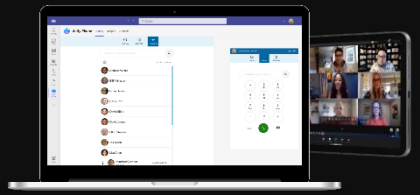


Unify OpenScape

Customers looking for an easy to use, native telephony soft client connected to OpenScape for exceptional mobile and hybrid working.

Unify Phone for Microsoft Teams

Available Now



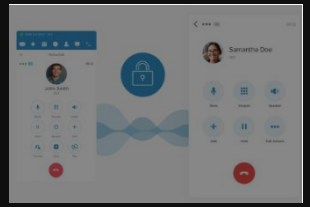
Microsoft Teams

Customers wanting continued benefit from their OpenScape telephony while adding a consistent Teams calling experience with a fully cloud based client.

Unify | NOW PART OF Mitel

Unify Phone
Google data center

Transmission Security

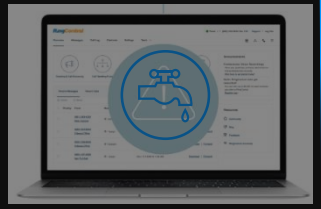


TLS 1.2/TLS 1.3 Encryption between all endpoints

Infrastructure Security

Access Control, Detection, Prevention & Monitoring

Proactive Fraud Mitigation



Throttling and Activity Detection

Physical & Environmental

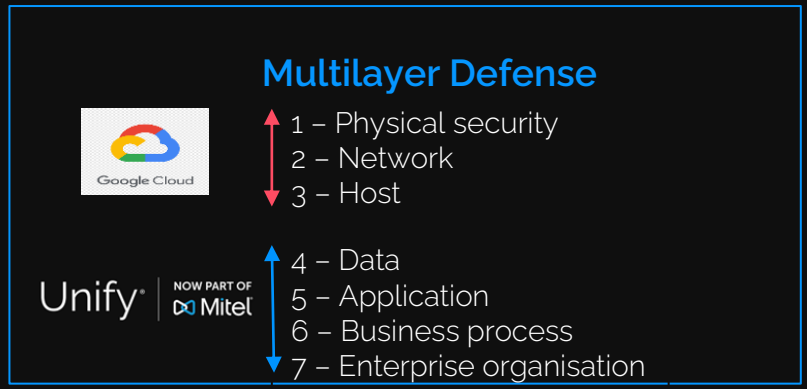
Audited accredited Data Centres – Google Cloud

Unify® | NOW PART OF Mitel®

Data Security and Privacy
7 layers of Security and Encryption

7 layers of security
- Unify Phone benefits from seven layers of security in-service operation.
- Physical access at the data centre, firewall and DDoS mitigation measures are secured by Google

Encryption
- Signalling protocols, data streams (DTLS) and media streams (SRTP)
- Data is encrypted at the transport layer (in transit)
- Data is encrypted while stored (at rest)



Unify | NOW PART OF Mitel

Data Security and Privacy
Frequently asked questions (FAQ)

What security do you have at data center?

We have 7 layers of security built into the service, so as an example for the Physical layer you DC access, and for Network you have Firewalls & DDoS mitigation measures

Is my organization's data encrypted in Unify Phone?

Data is encrypted at the transport layer and at rest

Can we offer PKI management with customer-specific keys/certificates?

We are unable to offer customers the ability to use/manage their own PKI keys for their instance.

What access rights are required for the mobile app?

When users install the Unify Phone mobile app for the first time, they are prompted to grant access to the inbuilt camera & microphone and to device contacts. During normal operation, it is apparent that the camera/microphone is on.

Encryption Elements of Unify Phone

Encryption in transit = YES

Transport layer encryption = YES

Encryption at rest = YES

Proprietary encryption = NO

Standards-based encryption = YES

End-to-end encryption = NO (but media and SIP signalling are secured)

Who is the Data privacy officer (DPO) for Unify Phone?

2 Data Protection Officer – GDPR (articles 13.1b /14.1b)
Unify has appointed a Data Protection Officer ("DPO").

Cloud Security Model – Security Concept

TLS, SRTP, REST

System Security

Isolation by KCS (Kubernetes Container Service)

Isolation of VM of the GCCE (Google Cloud Compute Engine)

Network Encryption

Clients

TLS encryption through GCP Web Load Balancer.

TLS1.2 & TLS1.3 and best-in-class Ciphers used.

PBX

TLS encryption for SIP

Media

SRTP to RTP Proxy

Other

TLS encryption to Mongo Atlas DB service

Network Security

Web Application

DDOS protection and Web Application Firewall by Google Cloud Armor

Client Authentication

Single Sign-On from Unify Office service over HTTPS connection

Database

Certificate Authentication to DB, generated by Google Secret Management

Data Encryption

Managing Mongo Atlas service in the GCP region of the Unify Phone deployment.

Encryption at Rest

Unify Phone Data and Security

Policies and Features within Unify Phone Controlled by the Tenant Administrator

- Data Retention
  - In accordance with the General Data Protection Regulation (GDPR),
  - You can export stored call data for users in your Unify Phone tenant.
  - You can also set how long data should be retained.
  - The default data retention period is 24 months
  - You can export call data for all users in your tenant in the last 24 months or in a selected date range. Data can be anonymized.

- Authentication
  - Unify Phone for Unify Video authenticates users using their Unify
    - Video account credentials.

  - Unify Phone for OpenScape can authenticate users in any of the following ways:
    - Unify Phone credentials: This is the default authentication
    - method. It uses internally stored credentials to authenticate users.
    - Single Sign On authentication: Single Sign On (SSO) allows users to sign in to Unify Phone using their corporate credentials.

Unify Phone
For more information

Terms of Service Production
https://unify.com/en/legal-information/unify-phone/terms-of-service-production

Privacy Policy
https://unify.com/en/legal-information/unify-phone/privacy-policy

Data Protection Policy
https://unify.com/en/legal-information/unify-phone/dpa

Unify Phone

Thank you!

Unify® | NOW PART OF Mitel®