PRIVACY AND SECURITY

We Offer Different Layers of Defense

Deltapath understands that privacy and security is a core business issue with any enterprise-grade, mission critical business platform. Our enterprise security and privacy approach protect the things that matter most to your company and users.

Over the last 20 years, Deltapath has designed, built and maintained a very secure Unified Communication (UC) solution. Our solution has been adopted across the world in different vertical markets, including but not limited to Banking & Finance, Government, Healthcare, Law Enforcement, Energy, Education, Manufacturing, Logistics, and Telecommunications.

The Deltapath product portfolio is developed and maintained in-house. System hardening and system integrity checks are conducted across our products to protect against file-based or malicious configuration threats, and to reduce the attack surface within products.

Layered Defenses

Deltapath follows a secure software development lifecycle (S-SDLC). Every phase of development ensures a high level of security that follows rigorous security requirements alongside functional requirements. The S-SDLC also places a significant emphasis on risk analysis and vulnerability management. To increase the security posture of Deltapath products, a defense-in-depth model is systematically incorporated through layered defenses:

- The principle of least privilege is always followed.
- Access is disabled or restricted to system accounts and those services that are nonessential to standard operation.
- Standards-based Static Application Security Testing (SAST) and patch management are cornerstones of our S-SDLC.
- Architecture reviews ensure compliance with requirements without conflicts, and validate the design quality, scalability, and performance of our products.
- Code reviews are implemented to detect issues prior to QA testing and limit the risk of introducing logic or design flaws, and common security misconfigurations that are hard to identify during the later phases of the SDLC process.
- Internal penetration testing and attack surface analysis are performed to verify the implementation of security controls across our products and regularly include:
    - Evaluating services on open TCP/UDP ports
    - Automated and scripted testing
    - Web UI testing (searching for XSS, CRSF, RCE, file inclusion, injections)
    - Evaluating access to and hardening of the underlying operating system in products
    - Manual testing and fuzzing of interfaces
    - Proactive testing of both our software solution and cloud platforms to ensure they do not introduce attack vectors to our customers' networks

A Holistic Approach

Take a closer look at Deltapath's holistic approach to protecting your business and your customers.

Operating System Security

The Deltapath operating system is a single user system. It does not allow execution of arbitrary code by any users. The entire operating system is encrypted offering additional security when it runs in any virtualized environment.

Architecture

Our architecture does not require any video conference room system, computer clients or mobile devices to have public WAN IP address or port forwarding enabled, reducing the threats of external attacks.

Authentication

Single Sign-On (SSO) with Microsoft Active Directory and LDAP helps to unify your corporate password policies. Reliable integration for SSO provides users with a seamless authentication experience. SSO adds a layer of security by empowering companies to control and customize any stage of the authentication and authorization process. That means your rules are always enforced.

Video and Audio Conference Meetings

Sensitive and confidential information is shared all the time in meetings. We make it harder for eavesdroppers and hackers to infiltrate your meetings and the sensitive data being communicated in your organization with advanced security features.

One-Time Guest Access

Most organizations take an open access approach with their conferencing systems where anyone with the dial in details can call in and access a meeting in progress. This approach opens companies to numerous vulnerabilities. Attackers can eavesdrop on meetings or read documents on conference room tables if someone forgets to change the last access code before the next meeting. Deltapath lets you create one-time meeting access codes for meeting participants to use from a regular telephone or a SIP URL from any SIP based video endpoint. The system validates the code before granting access to a caller. Once outside of the scheduled meeting time, the code is no longer valid. No one can get into your meeting unless invited.

Secure Information Flow

HTTPS

Feel confident when you see the padlock icon and HTTPS in a URL bar. Information exchanged over Deltapath's UC web interface supports HTTPS with SSL Certificate management. Data such as logins, passwords, and other personal information are all secure and encrypted. In addition, SSL certificates also provide authentication, which ensures the information you send goes to the right server.

Communications

An organization's communication data is mission-critical and sensitive. To protect your privacy, we enforce encryption on transit as well as in data storage if any of the communication is recorded for compliance purposes.

Session Initiation Protocol (SIP) Over Transport Layer Security (TLS)

The SIP TLS ensures call details such as caller ID and destination are encrypted. Every caller's connection is encrypted using single-use encryption keys.

Advanced Encryption Standard (AES)

All data and files sent using Deltapath's instant messaging tool use 256-bit AES encryption.

Call Recordings

Call recording file names are randomized to reduce the chances of them being discovered when inadvertently stored in online public drives.

Secure Real-Time Transport Protocol (SRTP)

SRTP is another protection tier that encrypts audio and video conversations. Media uses different ports for each call and is encrypted via SRTP/AES-128

Virus and Malware Detection

To protect the devices you send information to, an antivirus tool is used to ensure the files you send or receive over instant messages are virus free.

Encryption Technologies Used

- Server-to-server communication 256-bit AES-CBC for internal communications across our platform
- SHA 512 hashing for system file integrity monitoring
- 4096-bit Diffie-Hellman modulus for key exchange
- 256-bit AES CBC for data storage
- DTLS-SRTP for WebRTC media
- SRTP for SIP media
- SIP TLS for call signaling
- H.235 for H.323 media

Encryption for Mobile Users

Encryption on Deltapath® Mobile and Polycom® RealPresence Desktop is enforced. Encryption can be turned on for Polycom®/Poly® endpoints placed in external locations that will communicate over public internet.

Firewall

Deltapath offers a built-in firewall that automatically filters malicious packets. Similarly, the built-in SIP application firewall inspects and monitors all SIP dialogue exchanges between the public Internet and our server. Attacks such as brutal force attempts, number guessing, or application layer denial-of-service attacks are quickly filtered by the application firewall.   At all times, the topology of your network is masked and protected from external parties.

With the firewall security control and dynamic IP blocking tools, you can directly connect Deltapath UC to the internet securely even without any external firewall/security. We have implemented:

- DOS attack automatic rate control
- Malicious packet filtering
- Session aware firewall
- Automatic blacklist by source IP

Access Control

Licensed users can be assigned one of three roles in Deltapath's unified communications platform.

Super Privileges

This ACL group has the highest access level. As a result, any users with Super privileges can view, modify, and change user settings within the co-Super privileges and those users under Manager and Limited. Users with Super privileges can upgrade/downgrade users' ACL privileges to co-Super, Manager, and Limited.

Note: Co-Super refers to users/accounts on the same ACL privilege as Super privilege.

Manager

This ACL group can modify and view other user settings (extensions, number settings, etc.) with Limited and its co-Manager, but this group cannot view or modify individuals with Super privileges. In addition, anyone under the same Manager privileges cannot modify or upgrade their own or other co-Managers' ACL privilege to Super privileges. Anyone with Manager privileges can upgrade users with Limited privilege to Manager privilege only.

Note: Co-Manager refers to users/accounts on the same ACL privilege as Manager privilege.

Limited

This group has Limited privileges and cannot modify or view other user settings (extensions, number settings, etc.) with Manager, Super and its co-Limited privileges. In addition, anyone under this privilege cannot modify, view other users, or upgrade their own ACL privilege to Manager or Super privileges.

Detail System Logs and Audit Trial

Have access to security relevant, chronological records. Access all call history logs. View action executed by users in an audit trail.

About Deltapath

Deltapath liberates organizations from the barriers that prevent effective communication and revolutionizes the way organizations communicate through innovative technologies that meet the needs and the wants of organizations.

We specialize in solutions that unite different communication platforms, audio and video equipment, telephones, desktops, and mobile devices to make communication accessible and intuitive.

It is our belief that every solution should embody simplicity and offer users the right form of communication for the right occasion, right at their fingertips.

Ordering Information

For more information about Deltapath Privacy and Security, please contact your nearest Deltapath sales representative.

Deltapath

USA	+ 1 408 707 3299
NZ	+ 64 9 886 9799
HK	+ 852 3678 9999
JP	+ 81 3 3527 7899
TW	+ 886 2 7728 3099
PH	+ 63 2 8790 0295

www.deltapath.com