隐私和安全

我们为您提供多重防御

Deltapath 明白，隐私和安全是所有企业级和关键业务平台的核心业务问题。我们的企业安全和隐私保护方法将为您企业及用户的重要事项提供保护。

在过去 20 年，Deltapath 设计、构建和维护了一个非常安全的统一通信解决方案。我们的解决方案已在世界各地的不同纵向市场中得到采用，包括但不限于银行与金融、政府、医疗保健、执法、能源、教育、制造、物流和电信等行业。

Deltapath 产品组合经过内部开发和维护。我们通过检查所有产品的系统强化和系统完整性，从而防御基于文件或恶意配置的威胁，并减少产品内部的攻击面。

分层防御

Deltapath 遵循安全的软件开发生命周期（S-SDLC）。每个开发阶段均严格遵守安全和功能要求，以确保高水平的安全性。 S-SDLC 亦十分重视风险分析和漏洞管理。为了提高 Deltapath 产品的安全性，我们通过分层防御有系统地组成纵深防御模型：

- 始终遵循最小特权原则。
- 对系统管理账户及与标准操作无关的服务设置禁止或限制访问权限。
- 基于标准的静态应用程序安全测试（ SAST ）和补丁管理是我们 S-SDLC 的基石。
- 架构审查可确保无分歧地符合要求，并验证我们产品的设计质量、可扩增性和性能。
- 实施代码审查以在质量检查测试前发现问题，并降低引入逻辑或设计缺陷及在 SDLC 后期难以识别的常见安全性错误配置的风险。
- 执行内部渗透测试和攻击面分析以验证我们产品的安全控制措施的实施情况，通常包括：
    - 在开放的 TCP / UDP 端口上评估服务
    - 自动化和脚本化测试
    - 网页用户界面测试（搜索 XSS 、 CRSF 、 RCE 、包含文件、注入）
    - 对产品中底层操作系统的访问评估及强化
    - 手动测试和模糊界面
    - 主动测试我们的软件解决方案和云端平台，以确保它们不会将攻击媒介引入客户的网络

一个全面的方法

仔细了解 Deltapath 全面保护您业务和客户的方法。

操作系统安全性

Deltapath 操作系统是一个单用户系统，它不允许任何用户执行任意代码。整个操作系统经过加密，在任何虚拟环境中运行时均可提供额外的安全性。

架构

我们的架构不需要任何视频会议室系统、电脑客户端或移动设备使用 WAN IP 地址或端口转发，从而减少了外部攻击的威胁。

认证

具有 Microsoft Active Directory 和 LDAP 的单点登录 (SSO) 有助于统一企业密码政策。 SSO的可靠集成为用户提供无缝的身份验证体验。SSO通过授权企业控制和自定义身份验证及授权过程的任何阶段，为您再增加一层防御。这意味着您的规则将始终被执行。

视频和语音会议

会议期间经常需要共享敏感和机密信息。通过高级安全功能，窃听者和黑客很难渗透您的会议以及正在企业中传输的敏感数据。

一次性访问

大多数企业在其会议系统中采用开放式访问，任何拥有呼入信息的人都可以拨号并进入正在举行的会议。这种方法使企业面临许多漏洞，如果忘记在下一次会议之前更改上次的会议密码，攻击者就能轻易窃听会议或阅读会议室桌子上的文件。Deltapath允许您创建一次性会议访问代码，供会议参与者从普通电话使用，也可以从任何基于 SIP 的视频终端使用 SIP URL。系统在授予来电者访问权限前会先验证代码，一旦超出了预定的会议时间，该代码将失效。除非被邀请，否则任何人都不能参加您的会议。

Deltapath

安全信息流

HTTPS

在网址栏中看到挂锁图标和 HTTPS 时，请放心。通过 Deltapath 的 UC 网络界面交换的信息支持带有 SSL 证书管理的 HTTPS。诸如登录名、密码和其他个人信息之类的数据都是安全和经过加密的。此外，SSL 证书还提供身份验证，以确保您发送的信息到达正确的服务器。

通信

企业的通信数据至关重要且包含敏感资料。为了保护您的隐私，如果出于合规目的而要记录任何通信，我们将在传输以及数据存储中实施加密。

基于 TLS 的 SIP 协议

SIP TLS 确保对通话信息（例如来电者 ID 和目的地）执行加密。每通电话连接都使用一次性加密密钥执行加密。

高级加密标准（AES）

所有使用 Deltapath 即时通信工具发送的数据和文件均使用 256 位 AES 执行加密。

通话录音

通话记录文件名会被随机分配，以减少无意中将它们存储在公共存储器中时被发现的可能性。

安全实时传输协议（SRTP）

SRTP 是另一个加密语音和视频通话的防御机制。媒体为每通电话使用不同的端口，并通过 SRTP / AES-128 执行加密

病毒和恶意软件检测

为了保护传送信息的设备，我们采用了防病毒工具用于确保通过即时消息发送或接收的文件没有病毒。

使用的加密技术

- 服务器到服务器通信 256 位 AES-CBC：用于在我们平台上的内部通信
- SHA 512 哈希：用于系统文件完整性监视
- 4096 位 Diffie-Hellman 模组：用于密钥交换
- 256 位 AES CBC：用于数据存储
- 用于 WebRTC 媒体的 DTLS-SRTP
- 用于 SIP 媒体的 SRTP
- 用于呼叫信令的 SIP TLS
- 用于 H.323 媒体的 H.235

移动用户加密

在 Deltapath® Mobile 和 Polycom® RealPresence Desktop 上强制执行加密。可以在放置于外部位置并通过公共互联网通信的Polycom®/Poly® 终端执行加密。

防火墙功能

Deltapath提供了一个内置防火墙，可以自动过滤恶意数据包。同样，内置的 SIP 应用防火墙检查并监视公共互联网与我们的服务器之间的所有 SIP 会话。应用防火墙可以快速过滤诸如暴力攻击、数字猜测或应用层拒绝服务攻击之类的攻击。在任何时候，您的网络架构都被隐藏，并受到保护。

使用防火墙安全控制和动态IP 封锁工具，即使没有任何防火墙/安全设施，您也可以直接将 Deltapath UC 安全地连接到互联网。我们已经实现了：

- DOS攻击自动速率控制
- 恶意数据包过滤
- 会话感知防火墙
- 攻击源 IP 自动列入黑名单

访问控制

可以为获得许可的用户分配 Deltapath 统一通信平台中的三个角色之一。

超级权限 (Super Privileges)

此 ACL 组别具有最高的访问权限。任何具有超级权限的用户都可以查看、修改和更改其他超级权限用户 (co-Super) 、管理员和受限用户的设置。具有超级权限的用户可以将用户的 ACL 权限升降为超级权限、管理员和受限用户。

注：*Co-Super 是指与超级权限 (Super privilege) 用户拥有相同 ACL 权限的其他用户。*

受限用户 (Limited)

此组别只有有限的权限，并且不能修改或查看使用超级权限、管理员或其他受限用户的设置（例如分机号、号码设置等）。此外，此组别的用户都不能修改、查看其他用户，或将自己的 ACL 级别升级为管理员或超级权限。

管理员 (Manager)

此 ACL 组别可以修改和查看其他管理员和受限用户的设置（例如分机号、号码设置等），但是此组别不能查看或修改超级权限用户的设置。此外，任何拥有相同管理员权限的人 (co-Manager) 都不能将自己或其他管理员的 ACL 权限修改或提升为超级权限，但可以将受限用户升级为管理员。

注：*Co-Manager 是指与管理员 (Manager) 用户拥有相同 ACL 权限的其他用户。*

详细的系统日志和审计追踪

可以访问与安全性相关及按时间顺序的记录。访问所有呼叫历史记录日志。查看用户在审计追踪中执行的操作。

关于 Deltapath

Deltapath 将企业从阻碍有效通信的藩篱中解放出来，并通过创新的技术，满足企业所需所想，革新企业的通信方式。

我们专注于将不同的通信平台、音频和视频设备、电话、台式机和移动设备整合在一起，通过这样的解决方案使通信变得容易且直观。

我们相信，每个解决方案都应体现简单之美，并为用户提供及时且触手可及的通信方式。

订购信息

如欲了解更多有关 Deltapath Acute Cloud 的资讯，请联系我们的 Deltapath 销售代表。

Deltapath

CN +86 21 8037 9566
HK +852 3678 9999
TW +886 2 7728 3099
USA +1 408 707 3299
NZ +64 9 886 9799
JP +81 3 3527 7899
PH +63 2 8790 0295

cn.deltapath.com