隱私與安全性

我們為您提供多重防禦

Deltapath 明白隱私和安全性是每一個企業體系非常關心的核心問題。我們的企業安全和隱私保護方案可以保護您的企業和用戶。

在過去 20 年，Deltapath 設計、構建和維護了一套非常安全的統一通信解決方案。 我們的解決方案已在世界各地的不同垂直市場中得到採用以及驗證，包括但不限於銀行與金融、政府、醫療保健、執法、能源、教育、製造、物流和電信。

Deltapath 產品組合是在內部開發和維護的。我們對所有產品進行了系統強化和系統完整性檢查，以防禦基於檔案或惡意配置的威脅，並減少產品內部的攻擊面。

層層設防

Deltapath 遵循安全的軟件開發生命週期（S-SDLC）。每個開發階段均嚴格遵守安全和功能要求，以確保高水準的安全性。S-SDLC 亦十分重視風險分析和漏洞管理。為了提高 Deltapath 產品的安全性，我們透過分層防禦有系統地組成縱深防禦模型：

- 始終遵守最低許可權原則。
- 禁用或限制存取系統帳戶以及與基本操作無關的服務。
- 基於標準的靜態應用程式安全測試（SAST）和修補程式管理是我們 S-SDLC 的基石。
- 架構審查可確保無分歧地符合要求，並驗證我們產品的設計品質、可擴增性和性能。
- 貫徹代碼審查機制以在進行品管檢測前發現問題，並減低引入邏輯或設計缺陷以及在 SDLC 後期難以識別的常見安全性錯誤設置的風險。
- 執行內部滲透測試和攻擊面分析以驗證我們產品的安全控制措施之實施情況，並定期包括：
    - 在開放的 TCP / UDP 埠上評估服務
    - 自動化和腳本化測試
    - 網絡用戶界面測試（搜索 XSS、CRSF、RCE、檔案包含、注入）
    - 評估產品中底層操作系統的存取及進行強化
    - 手動測試和模糊介面
    - 主動測試我們的軟體和雲端平台，以確保它們不會將攻擊媒介引入客戶的網絡

全方位的保護

詳細瞭解 Deltapath 的全方位保護方案，全面保護您的企業和客戶。

作業系統安全性

Deltapath 採用單一用戶作業系統，它不允許任何使用者執行任意代碼。整套作業系統經過加密，以確保系統運作在任何虛擬環境中均可提供額外的安全性。

架構

在我們系統的整體架構中，網際網路 IP 地址或通訊埠轉發不是絕對必要的條件，進而減少了從外部而來的攻擊以及威脅。

認證方式

若您的企業本身具有 Microsoft Active Directory 和 LDAP 的單一簽入（SSO），有助於集中管理的企業密碼政策。 SSO 的可靠整合為用戶提供無縫的身份驗證體驗。SSO 通過授權企業控制和自定義身份驗證及授權過程的任何階段，為您再多增加一層防護。

視訊和語音會議

會議期間經常會需要共享企業的敏感或機密訊息。透過高階安全功能，駭客很難滲透到您的會議中以竊取會議中傳達的敏感數據。

一次性訪客存取權

大多數企業在其會議系統中採用開放的存取方式，代表著曾經存取過的訪客都可以致電並訪問正在進行中的會議。 這種方法使得企業會議系統面臨許多漏洞，假使有人忘記在下一次會議之前更改上次的訪問密碼，攻擊者便能輕易竊聽會議或讀取會議中分享的敏感文件。Deltapath 提供您建立一次性會議訪問代碼，供會議參與者從一般電話系統使用，也可以從任何基於 SIP 的視訊終端設備使用 SIP URL 參與會議。系統在授予來電者訪問權限前會先驗證代碼，一旦超出了預定的會議時間，該代碼將失效。除非被邀請，否則任何人都不能參加您的會議。

Deltapath

安全信息流

HTTPS

在網址列中看到掛鎖圖示和 HTTPS 時，請放心。通過 Deltapath 的 UC 網絡介面交換的信息支援帶有 SSL 證書管理的 HTTPS，帳號、密碼和其他個人信息等數據都是安全和經過加密的。 此外，SSL 證書還提供身份驗證，以確保您發送的信息能到達正確的伺服器。

通信

企業的通信數據至關重要且包含敏感資料。為了保護您的隱私，如果出於合規目的而要記錄任何通信，我們將在傳輸以及數據存儲中實施加密。

傳輸層安全性（TLS）上的對話啟動協定 (SIP)

SIP TLS 確保對通話信息（例如來電者 ID 和目的地）進行加密。每通電話連接都使用一次性加密密鑰進行加密。

高階加密標準（AES）

所有使用 Deltapath 即時通訊工具發送的數據和文件均使用 256 位 AES 進行加密。

通話錄音

通話記錄檔案名稱會被隨機分配，以減少無意中將它們存儲在網路公共硬碟中時被發現的可能性。

安全即時傳輸協定（SRTP）

SRTP 是另一個加密語音和視訊通話的防護層。系統為每一通電話每一個媒體流分派不同的連接埠，並通過 SRTP / AES-128 進行加密

病毒和惡意軟件檢測

為了保護傳送訊息的裝置，防毒工具用於確保通過即時通訊發送或接收的檔案皆沒有病毒威脅。

使用的加密技術

- 伺服器到伺服器通信 256 位 AES-CBC，用於在我們平台上進行內部通信
- SHA 512 雜湊演算法用於監控系統檔案的完整性
- 4096 位迪菲－赫爾曼模指數用於密鑰交換
- 256 位 AES CBC 用於數據存儲
- 用於 WebRTC 媒體的 DTLS-SRTP
- 用於 SIP 媒體的 SRTP
- 用於呼叫信令的 SIP TLS
- 用於 H.323 媒體的 H.235

行動用戶加密

在 Deltapath®Mobile 和 Polycom®RealPresence Desktop 上強制執行加密。可以在放置於外部位置並通過公共網際網路進行通信的的 Polycom®/Poly® 終端設備執行加密。

防火牆功能

Deltapath 系統內建防火牆，可以自動過濾惡意數據包。 同樣，內建的 SIP 應用程式防火牆會不斷地檢查並監控網際網路與 Deltapath 伺服器之間的所有 SIP 對話交換。 應用程式防火牆可以快速過濾暴力破解法、數字猜測或應用程式層阻斷服務攻擊之類的攻擊。不論何時，企業的內部網絡結構都被隱蔽，並受到保護。

使用防火牆安全控制和不斷變化的 IP 封鎖工具，即使沒有任何外部防火牆/保安措施，您也可以直接將 Deltapath UC 安全地連接到網際網路。 我們已經實現了：

- DOS 攻擊自動速率控制
- 惡意數據包過濾
- 會話感知防火牆
- 依據來源 IP 自動列入黑名單

存取控制層級

可以為所有使用者個別分配 Deltapath 統一通信平台中的三個角色權限組。

最高管理權

此 ACL 組別具有最高的存取權限。此權限的使用者可以查看、修改和更改其他相同層級的使用者以及更低層級的管理員和受限制使用者的設置。最高管理權的使用者可以提高或降低所有使用者的 ACL 權限組。

受限制使用者

此組別只會被分配到有限制的權限，並且不能修改或查看所有其他使用者的設置（例如分機號、號碼設置等）同樣地也不能提高或降低所有其他使用者的管理權限組。

管理員

此 ACL 組別可以修改和查看其他水平層級或更低層級的使用者配置（例如分機號、號碼設置等），但是此組別不能查看或修改更高層級(最高管理權)的使用者配置。任何擁有管理員權限的人都不能將自己或其他管理員的 ACL 權限向上調整為最高管理權，但可以將受限制組別的使用者提高為與自己相同水平的管理員層級。

詳細系統日誌和審計追踪

可以存取與安全性相關及按時間順序的記錄。存取所有通話歷史記錄日誌。查看用戶在審計追踪中執行的操作。

關於Deltapath

Deltapath將企業從阻礙有效通信的障礙中解放出來，並通過能滿足企業需求的創新技術革新企業的通信方式。

我們專注於將不同的通信平台、音頻和視頻設備、電話、桌上型 電腦和移動設備結合在一起的解決方案，以使通信變得容易且直觀。

我們相信每個解決方案都應體現簡單性，並在適當的時候給用戶提供觸手可及的通信方式。

訂購信息

如想了解更多有關 Deltapath 統一通信平台的信息，請聯繫您就近的 Deltapath 銷售代表。

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

tw.deltapath.com