TeamViewer 安全資訊

目標群體

本文檔的目標群體是專業網路管理員。本文檔提供的資訊屬於技術資訊且非常詳盡。根據這些資訊，IT 專業人員將全面詳細地瞭解 TeamViewer 的安全標準，並在部署軟體之前解決所有問題。您可以隨時將此文檔分發給客戶，以減少任何可能發生的安全問題。

如果您認為自己不屬於本文檔的目標群體，「公司/軟體」部分提供的資訊仍然可以幫助您清楚地瞭解我們如何認真對待安全問題。

公司/軟體

關於我們

TeamViewer GmbH 成立於 2005 年，總部位於德國南部的哥廷根（在斯圖加特附近），在澳大利亞和美國設有子公司。我們專門開發和銷售用於網上協作的安全系統。我們的免費增值授權模式使我們在短時間內得到迅速發展，目前有 2 億多使用者在 14 億台設備上使用 TeamViewer 軟體，遍及全球 200 多個國家。該軟體有 30 多個語言版本。

我們對安全的理解

在任何一天的任何時候，都有 3000 多萬使用者正在使用 TeamViewer。這些使用者正在網際網路上提供自發的支援、使用無人值守的電腦（即伺服器的遠端支援）以及舉行線上會議。根據配置，TeamViewer 可用於遠端控制另一台電腦，就像您直接坐在電腦前面一樣。如果登入遠端電腦的使用者是 Windows、Mac 或 Linux 管理員，他們也將擁有遠端電腦的管理員權限。

很明顯，在可能不安全的網際網路上授予這樣強大的功能，必須透過嚴格的審查進行保護，以免受攻擊。實際上，安全問題在我們的所有發展目標中佔有重要地位，我們所做的一切都非常注重安全問題。我們希望確保您能安全地使用我們的電腦並保護我們自己的利益：數以百萬計的全球使用者只信任安全的解決方案，只有安全的解決方案才能確保我們的企業取得長遠成功。

品質管制

根據我們的理解，如果沒有既定的品質管制體系，不可能實現安全管理。TeamViewer GmbH 是市場上為數不多的實施 ISO 9001 認證品質管制體系的供應商之一。我們的品質管制遵循國際公認的標準。我們每年都透過外部審計來審查品質管制體系。

外部專家評估

我們的軟體 TeamViewer 已經被聯邦資訊技術專家和評審員協會（Bundesverband der IT-Sachverständigen und Gutachter e.V.，簡稱 BISG e.V.）授予五星品質標誌（最高級別）。BISG e.V. 的獨立評審員檢查合格生產商的產品品質、安全和服務特點。

參考資料

目前，有超過 2 億使用者使用 TeamViewer。來自各行各業的國際頂級企業（包括銀行、金融、醫療和政府等高度敏感的行業）都在成功地使用 TeamViewer。

我們邀請您查看在網際網路上隨處可見的關於我們的參考資料，初步瞭解客戶如何接受我們的解決方案。您會發現，大概大部分其他公司都有相似的安全性和可用性要求，他們經過深入考察，最終決定使用 TeamViewer。為了讓您進一步瞭解我們的軟體，請查看本文檔其餘部分提供的技術細節。

TeamViewer 會議

創建會話和連接類型

在建立會話時，TeamViewer 會確定最佳連接類型。透過主要伺服器握手後，在所有情況下，70% 會透過 UDP 或 TCP 建立直接連接（甚至在標準閘道、NAT 和防火牆之後）。其餘連接透過 TCP 或 https 通道的高冗餘路由器網路進行路由。您不必為了使用 TeamViewer 而打開任何埠

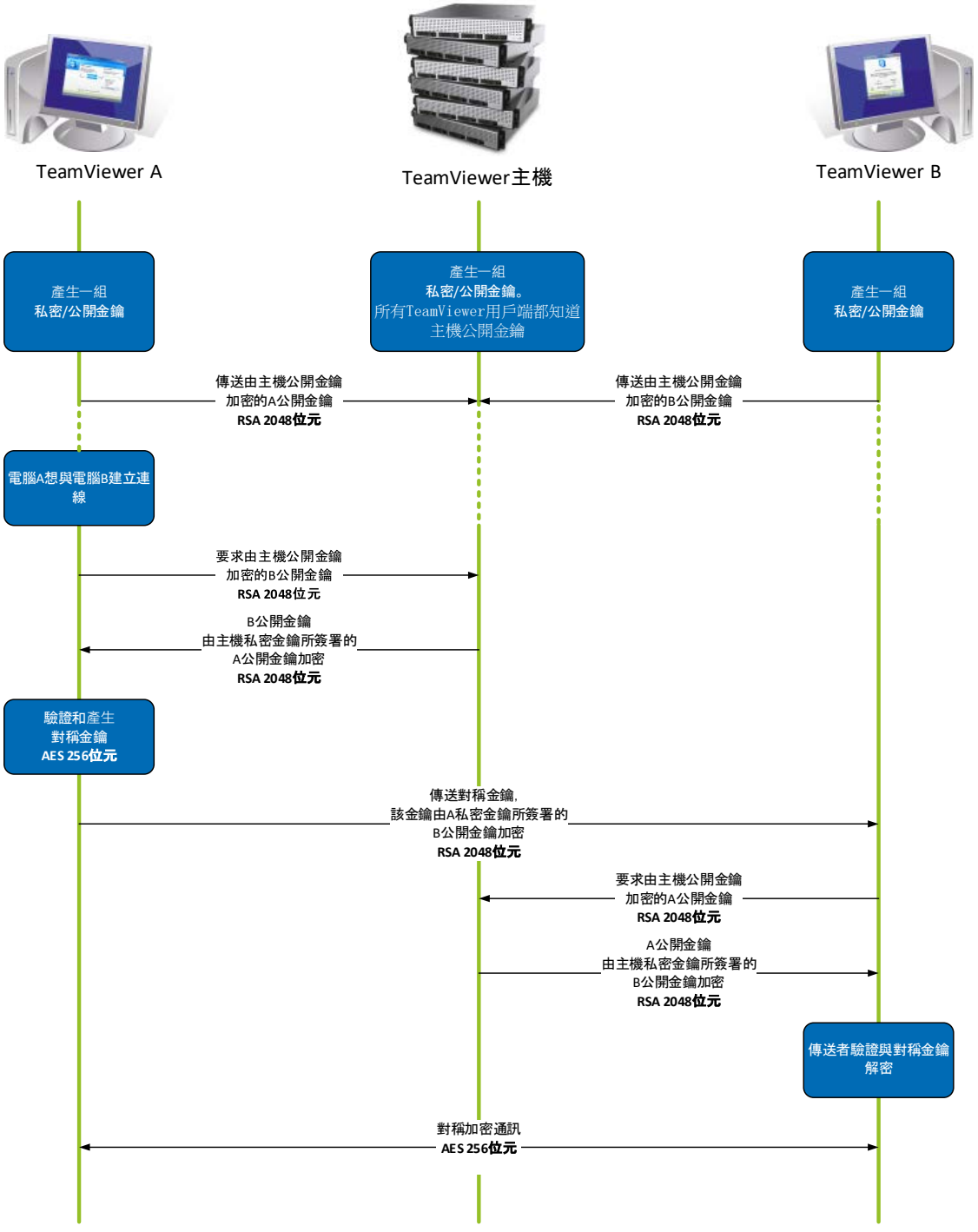
後面將在加密和驗證一段說明，即使我們作為路由伺服器營運商，也不能讀取加密的資料通信。

加密和驗證

TeamViewer 通信使用 RSA 公開金鑰/私密金鑰交換和 AES（256 位）會話加密來保護。該技術以 http/SSL 的可比較形式使用，現行標準認為該技術完全安全。由於私密金鑰永遠不會離開用戶端電腦，因此，該程序可確保互連的電腦（包括 TeamViewer 路由伺服器）無法解密資料流。

每個 TeamViewer 用戶端已經實施了主集群的公開金鑰，因此可以將消息加密到主集群，並檢查由其簽名的消息。PKI（公開金鑰基礎設施）可有效防止中間人攻擊。儘管使用加密，但密碼永遠不會直接傳送，只能透過質詢-回應過程傳送，並且只儲存在本端電腦上。

在驗證過程中，由於使用安全遠端密碼 (SRP) 協定，密碼永遠不會直接傳輸。本端電腦上只儲存密碼驗證器。



TeamViewer 加密和驗證

TeamViewer ID 的驗證

TeamViewer ID 基於各種硬體和軟體特性，由 TeamViewer 自動生成。在每次連接之前，TeamViewer 伺服器會檢查這些 ID 的有效性。

蠻力保護

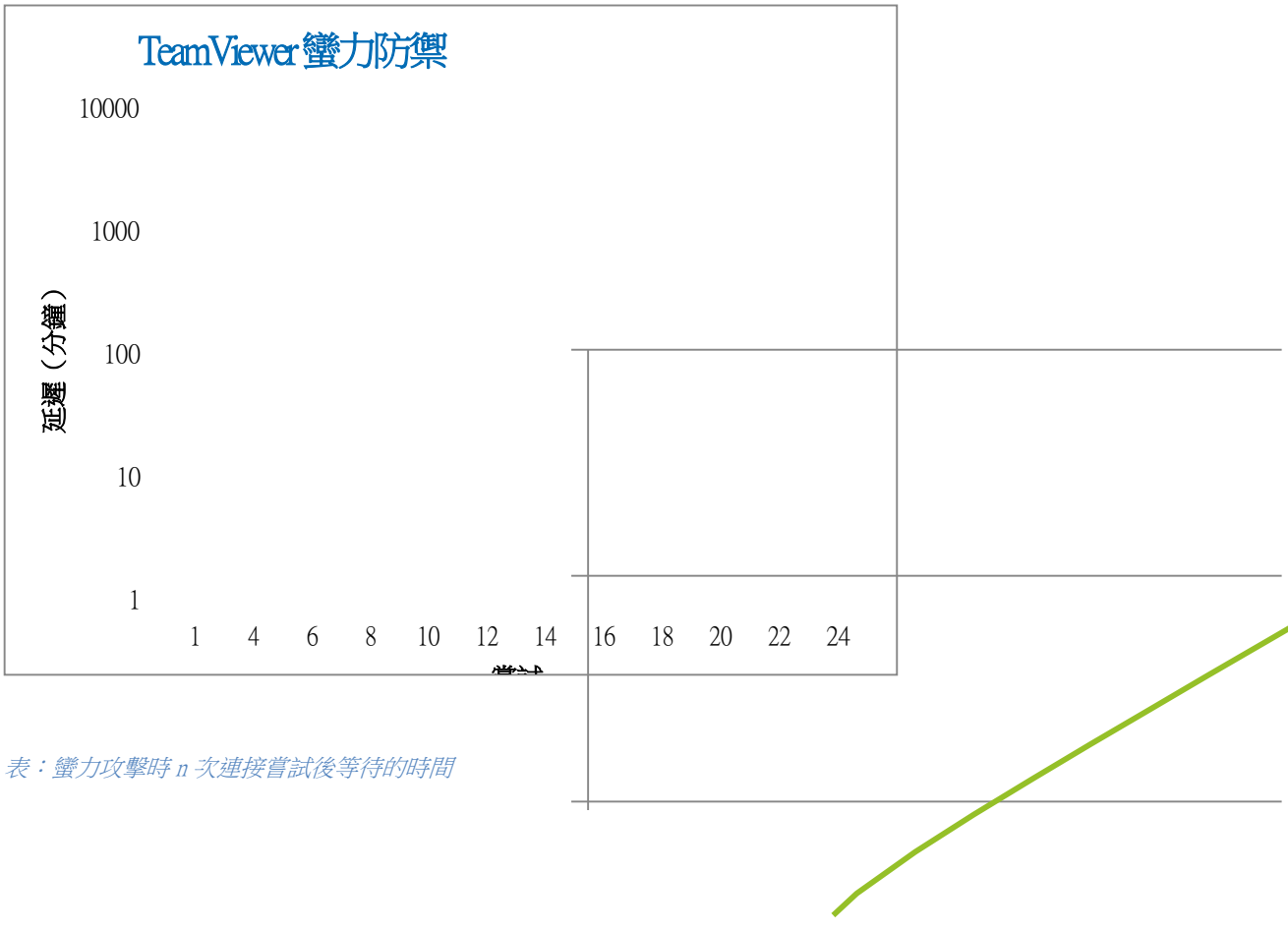
詢問 TeamViewer

安全性的潛在客戶經常詢問有關加密的資訊。我們可以理解，客戶最擔心第三方可以監視連接或 TeamViewer 存取資料被竊聽。然而，實際情況是非常原始的攻擊往往是最危險的。

在電腦安全領域，蠻力攻擊是使用試錯方法猜測用於保護資源的密碼。隨著標準電腦的計算能力不斷增強，猜測長密碼所需的時間不斷減少。

為了防止蠻力攻擊，TeamViewer 連接嘗試之間的延遲時間呈指數級增加。因此，24 次嘗試需要多達 17 個小時。只有成功輸入正確的密碼，延遲時間才會重置。

TeamViewer 不僅採用有效的機制來保護客戶免受一台特定電腦的攻擊，還可以防禦嘗試使用一個特定 TeamViewer ID 的多台電腦（稱為僵屍網路攻擊）。



表：蠻力攻擊時 n 次連接嘗試後等待的時間

代碼簽名

作為一項額外的安全功能，我們的所有軟體都透過 VeriSign 代碼簽名進行簽名。這樣，軟體的發行者總是易於識別。如果後來軟體被更改，數位簽名將自動變為無效。

資料中心和骨幹

為了使 TeamViewer 服務擁有最佳安全性和可用性，所有 TeamViewer 伺服器均位於符合 ISO 27001 標準的資料中心，並使用多冗餘營運商連接和冗餘電源。此外，我們只使用最先進的品牌硬體。另外，所有儲存敏感資料的伺服器均位於德國或奧地利。

通過 ISO 27001 認證意味著個人存取控制、攝像機監控、運動檢測器、24x7 監控和現場安全人員可確保資料中心的存取權只會授予經授權的人員，並保證硬體和資料的最佳安全性。資料中心的單個入口點還有詳細的識別檢查。

TeamViewer 賬戶

TeamViewer 賬戶託管在專用的 TeamViewer 伺服器上。有關存取控制的資訊，請參閱上面的資料中心和骨幹。針對授權和密碼加密，使用安全遠端密碼協定（SRP，增強的密碼-驗證金鑰協定 (PAKE)）。滲透者或中間人無法獲得蠻力猜測密碼所需的足夠資訊。這意味著即使客戶使用強度較弱的密碼也可以獲得很強的安全性。TeamViewer 賬戶中的敏感資料（例如雲端儲存登入資訊）使用 AES/RSA 2048 位元加密儲存。

管理主控台

TeamViewer 管理主控台是基於網路的平臺，用於使用者管理、連接報告以及管理電腦和聯絡人。它託管在經 ISO-27001 認證、符合 HIPAA 標準的資料中心。所有資料傳輸都透過使用 TSL（傳輸安全層）加密（網際網路安全連接標準）的安全通道。敏感性資料進一步使用 AES/RSA 2048 位元加密儲存。針對授權和密碼加密，使用安全遠端密碼協定 (SRP)。SRP 採用 2048 位元模數，是一種成熟、 穩健、安全且基於密碼的驗證和金鑰交換法。

基於政策的設置

在 TeamViewer 管理主控台中，使用者可以為專屬於他們的設備上安裝的 TeamViewer 軟體，定義、分配和執行設置政策。設置政策由生成政策的賬戶進行數位簽名。這可以確保能夠將政策分配給設備的唯一賬戶是設備所屬的賬戶。

TeamViewer 中的應用程式安全性

黑名單和白名單

特別是如果 TeamViewer 用於維護無人值守的電腦（即 TeamViewer 作為 Windows 服務安裝），那麼將這些電腦的存取權限制為多個特定用戶端的額外安全選項可能很有用。

使用白名單功能，您可以明確指出允許哪些 TeamViewer ID 和/或 TeamViewer 賬戶使用電腦。使用黑名單功能，您可以阻止某些 TeamViewer ID 和 TeamViewer 賬戶。中央白名單是上述「管理主控台」中「基於政策的設置」的一部分。

聊天和視頻加密

聊天記錄與您的 TeamViewer 賬戶相關聯，因此使用與「TeamViewer 賬戶」標題下所述的相同的 AES/RSA 2048 位元加密安全方法進行加密和儲存。所有聊天消息和視頻通信都使用 AES（256 位元）會話加密進行端對端加密。

沒有隱身模式

沒有能夠讓 TeamViewer 完全在後臺運行的功能。即使應用程式作為 Windows 服務在後臺運行，始終可以透過系統託盤中的圖示看到 TeamViewer。

建立連接後，系統託盤上始終能看到一個小控制台。因此，TeamViewer 被有意設計為不適合隱蔽地監控電腦或員工。

密碼保護

對於自發的客戶支援，TeamViewer (TeamViewer QuickSupport) 生成會話密碼（一次性密碼）。如果您的客戶告訴您他們的密碼，您可以透過輸入他們的 ID 和密碼連接到他們的電腦。在客戶一端重新開啟 TeamViewer 後，將生成新的會話密碼，因此，您只有獲得邀請，才能連接到客戶的電腦。

如果部署 TeamViewer 用於無人值守的遠端支援（例如伺服器的遠端支援），您可以設置單獨的固定密碼，以保護對電腦的存取權。

傳入和傳出存取控制

您可以單獨配置 TeamViewer 的連接模式。例如，您可以配置您的遠端支援或會議電腦，使其不能建立傳入連接。

將可用功能限制為實際需要的功能，總是意味著可以限制可能被攻擊的潛在弱點。

雙因素驗證

TeamViewer 協助公司實施 HIPAA 和 PCI 合規要求。雙因素驗證增加一個額外安全層，以保護 TeamViewer 賬戶不接受未經授權的存取。

除了使用者名稱和密碼之外，使用者必須輸入代碼才能進行驗證。該代碼透過基於時間的一次性密碼 (TOTP) 演算法生成。因此，代碼僅在短時間內有效。

透過雙因素驗證以及使用白名單限制存取權，TeamViewer 有助於滿足 HIPAA 和 PCI 認證的所有必要條件。

安全測試

TeamViewer 基礎架構和 TeamViewer 軟體均經常進行滲透測試。測試由專門從事安全測試的獨立公司執行。

其他問題？

若有任何問題或需要進一步的資訊，歡迎撥打下列號碼與我們聯絡：400 120 3143 (粵语) 與 +86 (0) 10 8418 1824 (粵语)，或是發送電子郵件寄至 support@teamviewer.com。

聯絡方式

TeamViewer GmbH
Jahnstr.30
D-73037 Göppingen
Germany
service@teamviewer.com