型錄

CLAROTY 安全遠端存取(SRA)

適用於工業網路的無阻礙、可靠且高度安全的遠端存取

工業網路遠端存取的挑戰

我們所打造的 Claroty SRA 可以解決營運技術(OT)遠端存取的挑戰。更特別的是，雖然 OT 遠端存取對工業企業極為重要，但三個關鍵原因使其長久以來客戶對於 OT 遠端存取功能仍有疑慮駐足不前：

1. 終端使用者的複雜性：增加 MTTR

大部分的傳統遠端存取工具都是針對 IT 網路所設計，具有繁瑣的存取機制和介面，因此無法滿足 OT 的需求。

終端使用者在使用這些工具之前，不僅需要進行冗長的上線和教育訓練—而且這些工具操作複雜且缺乏效率，表示無論使用者接受再多的教育訓練，仍可能難以滿足其盡快修復工業資產的需求。

這些情況會增加使用者的平均修復時間(MTTR)，這在必須立即修復才能避免或減少停機或其他嚴重後果的緊急狀況下，很可能會造成問題。

2. 管理複雜度：增加整體擁有成本(TCO)

內部和第三方使用者必須能夠在需要維護或另有目的時遠端存取工業資產。

如果要管理這種存取方式，系統管理員必須維護成本高昂的複雜基礎網路架構，同時解決使用者的上線和疑難排解需求。

尤其對於第三方使用者難以提供適切支援，因為他們通常無法和來自其他供應商的使用者共用跳板機或其他基礎網路架構，讓系統管理員面臨更複雜的問題。

此一過程費資耗時，讓傳統的遠端存取工具在 OT 環境使用的整體擁有成本(TCO)偏高。

3. 可視性與安全控制不佳：增加面臨的風險

OT 遠端使用者可能會進行未經授權的變更，致使營運面臨風險。這些風險會隨著使用傳統遠端存取工具變得更加複雜，因為這些工具無法讓網路安全人員完全掌握使用者的各項活動，而且無法讓此類人員對使用者實行角色型和原則式存取控制。

另一個顧慮是這類工具通常在本質上並不安全，因為這類工具通常使用易受攻擊的 RDP 通訊協定，而且違反普渡模型(Purdue Model)。其作法和工業網路安全最佳實務背道而馳，因此網路安全人員無法辨識和控制誰從何處、何時或為何登入。他們也無法辨識或回應和這些使用者活動相關的事件，這些事件全都會讓 OT 環境面臨更大的風險。

關於 Claroty SRA

Claroty SRA 可以提供無阻礙、可靠與高度安全的方式，讓內部和第三方使用者遠端存取 OT 環境，解決 OT 遠端存取所要面臨的挑戰。有別於大多數是針對 IT 網路單獨設計的傳統遠端存取解決方案，Claroty SRA 是專為工業網路特定作業、系統管理和資安需求所製作。結果是一項獨特的解決方案，可以縮短您的平均修復時間(MTTR)，將設定和管理您 OT 遠端使用者存取權限的成本和複雜度降到最低，以及減少您的 OT 環境面臨未經管理、未受控制和不安全存取所造成的風險。

SRA 的特性與功能

縮短 MTTR 的使用者體驗

SRA 可以降低終端使用者的 OT 遠端存取複雜度，讓使用者能夠在必要時以更輕鬆快速的方式存取、疑難排解，以及修復工業資產。產品特性包括：

- **及時(JIT)使用者佈建：**SRA 可以透過 SAML 及 OpenID Connect (OIDC)和各種身分識別供應商(IdP)整合，讓系統管理員可以將做為單一登入流程其中一部分的建立 SRA 使用者帳戶自動化與簡化。這表示新的使用者可以自動新增至 SRA 並立即開始使用，完全不需要系統管理員執行任何其他步驟。
- **高效率的驗證及存取：**SRA 也提供原生多重要素驗證。因此獲得授權的 SRA 使用者可以在緊要關頭，以快速且安全的方式進行驗證和取得存取權。
- **直覺的介面：**SRA 介面可直接反映使用者的原先使用者體驗，無需學習曲線或大量教育訓練，提供無可比擬的可用性。
- **高可用性：**SRA 內含高可用性機制，可確保使用者不論在哪種情況下均可維持存取。

主要特性與優點

- SRA 可讓您隨時隨地以更輕鬆快速的方式連線和修復 OT、物聯網(IoT)及工業物聯網(IIoT)資產，因此可以縮短 MTTR 並延長運作時間。
- SRA 提供靈活的設定選項、集中式管理，以及內部和第三方使用者所需的一切，藉此將無害、安全且可靠的 OT 遠端存取的複雜度與成本降低。
- SRA 讓您能夠控制、保護，以及完全掌握您網路中的所有遠端連線與活動，將 OT 遠端存取的風險降到最低。

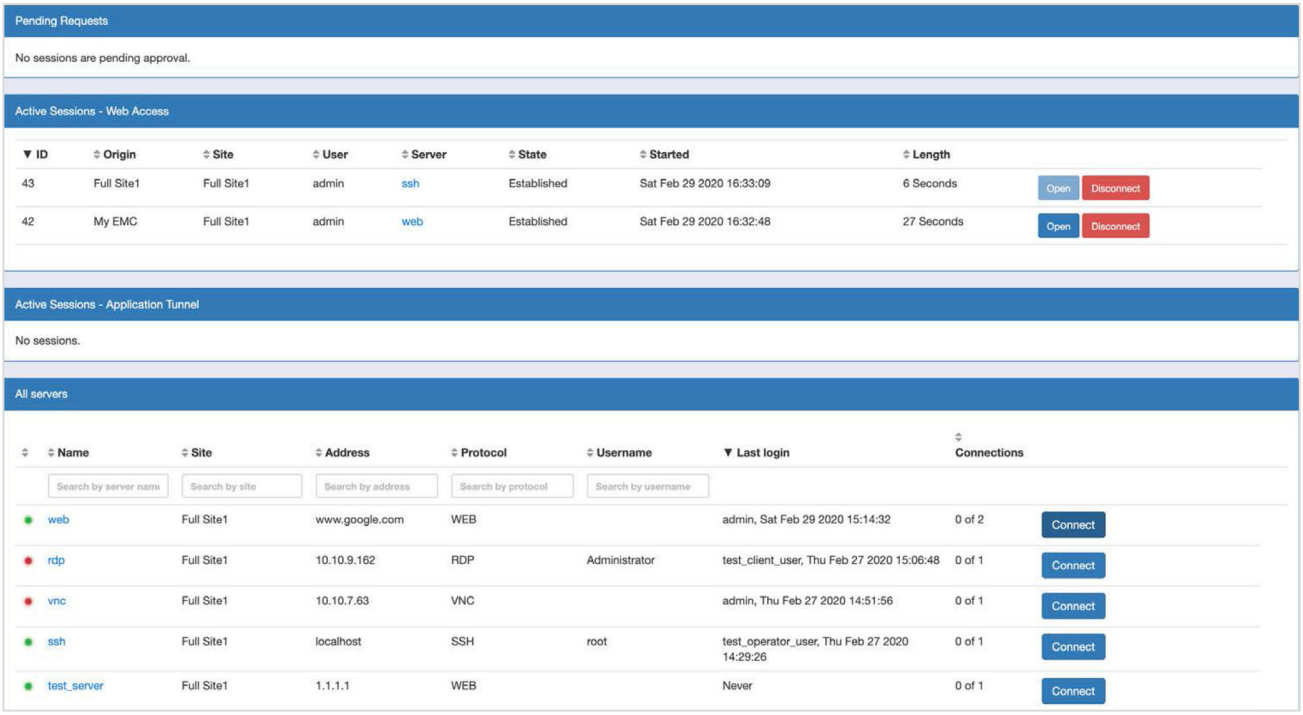

圖 1：使用遠端連線的 SRA 首頁視圖

可以減少管理 OT 遠端存取整體擁有成本(TCO)的管理功能

SRA 可以提供靈活的設定選項、集中式管理，以及內部和第三方使用者支援其 OT 遠端存取使用案例所需的一切，因此可以降低系統管理員在 OT 遠端存取上通常偏高的整體擁有成本(TCO)。產品特性包括：

- **及時(JIT)使用者佈建：**JIT 使用者佈建除了可以讓 SRA 使用者獲益，也可以將幾乎所有手動與耗時的佈建和保護存取流程，以及新的 SRA 使用者上線自動化，讓 SRA 系統管理員能夠節省大量的時間和資源。
- **靈活的部署和設定選項：**部署或設定 SRA 不需使用跳板機、複雜的防火牆規則，或是其他傳統遠端存取解決方案常見的通常成本高昂又複雜的架構元件。因此，SRA 系統管理員在部署和管理其使用者的遠端存取基礎網路架構時所需要的時間與金錢都較少，因此可以降低其整體擁有成本(TCO)。
- **完整支援所有 OT 遠端存取使用案例：**SRA 內含支援所有 OT 遠端存取使用案例所需的全方位特性與功能，因此是真正的一站式 OT 遠端存取解決方案。這些包括專為 OT 打造的使用者介面、多重要素驗證使用的多重選項、密碼保存庫、安全檔案管理、高可用性、全面監控等。這表示您不需要採購、部署和維護多個解決方案，即可滿足您內部和第三方使用者的 OT 遠端存取需求。

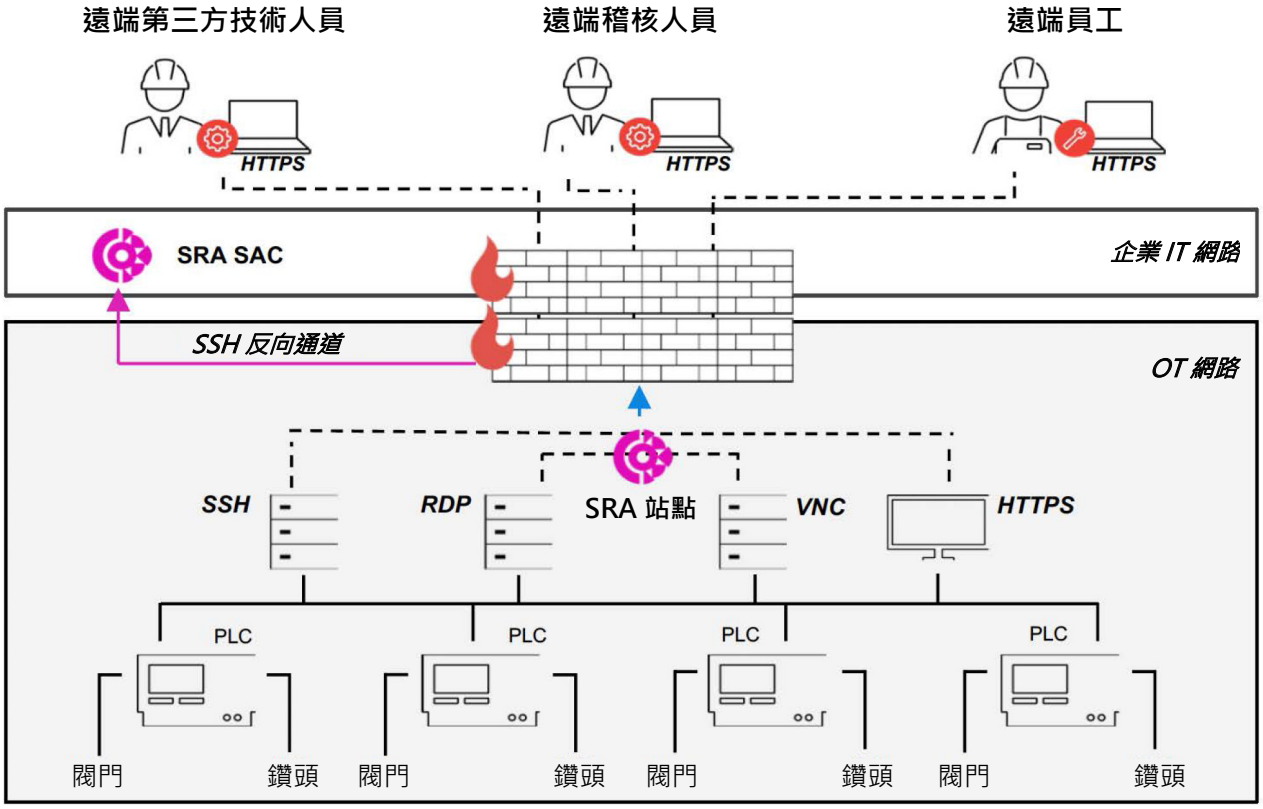

圖 2：SRA 範例部署架構-簡易設定可供多種類型遠端使用者使用

可將遠端使用者所造成的風險降到最低的存取及驗證控制

SRA 系統管理員可以利用特定方式控制對其跨多個層級工業網路的存取，以判斷誰可以存取哪些資產、採用哪種方式、存取時間、存取目的，以及透過哪些通訊協定。產品特性包括：

- **安全驗證：**SRA 內含原生多重要素驗證及認證管理選項、支援執行密碼有效性管理，並可提供與 SAML 和 OIDC 型身分識別供應商整合的能力。
- **與身分識別供應商整合：**選擇將系統和其現有身分識別供應商整合的 SRA 系統管理員，可以將已經在其企業組織執行的 SAML 或 OIDC 型驗證原則和密碼需求自動擴充到其 SRA 使用者帳戶，因此可以確保對 OT 員工和第三方使用者等進行高強度的使用者驗證。這項功能也可以讓前員工的 SRA 認證自動失效，因此可以排除常用於提權攻擊和密碼重複使用攻擊的高風險攻擊方式。

- **角色型和原則式存取：**SRA 系統管理員可以在多個層級和地理位置定義與執行極為精密的工業資產控制，最終可以簡化使用者的工作流程並防止重要功能遭到非必要的存取。此類控制支援零信任(Zero Trust)和最小權限(Least Privilege)的安全原則。
- **安全核准和緊急存取：**可以針對遠端存取時會構成安全風險的資產建立額外的原則，以確保每個資產所在地環境的健康情況和可操作性。

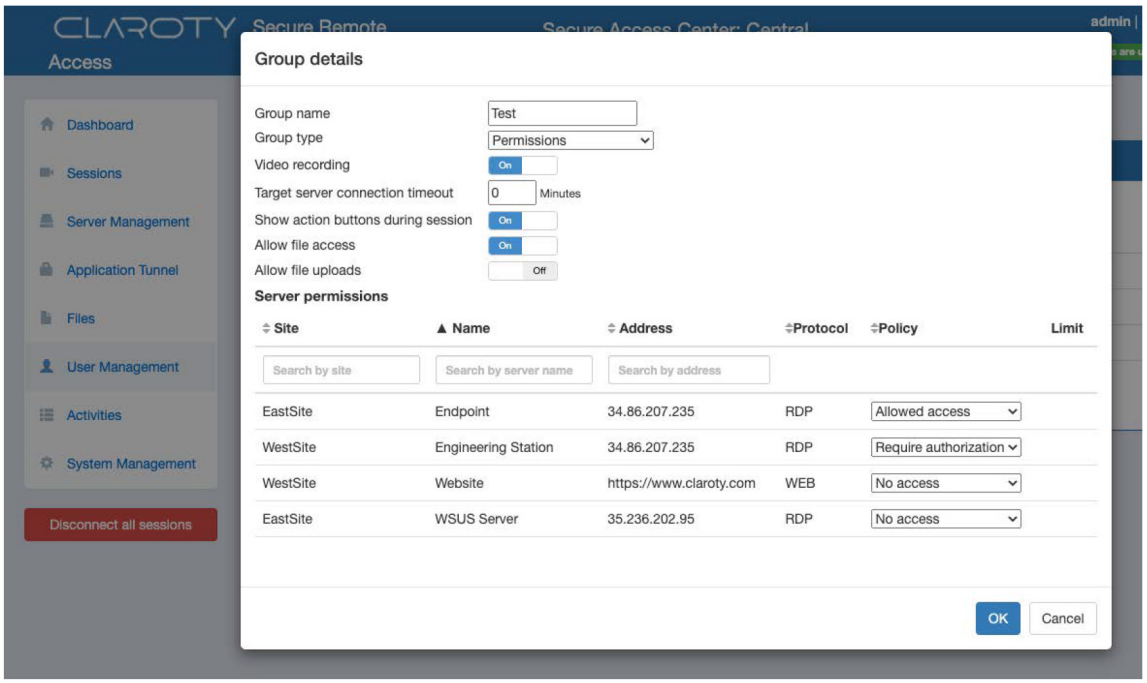

圖 3：SRA 內的群組詳細資料

可以減少攻擊面的本質安全架構與功能

將您工業網路中的重要資產與外部連結隔離以及惡意程式的主動防止，對於減少攻擊面並因此降低遠端使用者所造成的風險非常重要。SRA 可以透過以下方式提供這些功能：

- **對傳輸中的資料使用加密通道：**SRA 會將在兩個加密通道之間傳輸的資料進行分割，藉以減少連線網路的裝置數量和防火牆中開啟的連接埠數量，並因此而減少攻擊面。
- **保留普渡模型：**所有 SRA 部署選項均遵循保留普渡模型的工業網路安全最佳實務，因此有助於確保單一連線點，不會提供廣泛的網路存取。
- **與防毒解決方案整合：**SRA 可以和所有 ICAP 型防毒解決方案進行整合。這項功能可以提高在工業資產中執行遠端維護與相關工作所需上傳檔案的安全性，因此有助於防止您的工業網路受到惡意程式的攻擊。如果此類檔案為惡意檔案，系統會立即通知 SRA 使用者並防止使用者將其上傳至個別資產。

圖 4：SRA 的加密通道圖表

可以簡化稽核和優化調查的監控功能

SRA 可以提供遠超過傳統遠端存取技術所提供的基本登入功能和有限稽核軌跡，因此可以讓您取得最完整即時的 SRA 使用者活動可視性、簡化稽核以及優化事件調查。

產品特性包括：

- **即時的全面監控：**SRA 系統管理員可以選擇即時監控作用中的 SRA 工作階段，因此可以在認為必要時輕鬆進行疑難排解、使用者監督，並且緊急終止高風險的工作階段。
- **完整長度的視訊記錄：**除了保留所有遠端工作階段的詳細記錄，SRA 還會自動記錄每個工作階段的完整長度視訊，以便為回應動作、調查與稽核提供支援。

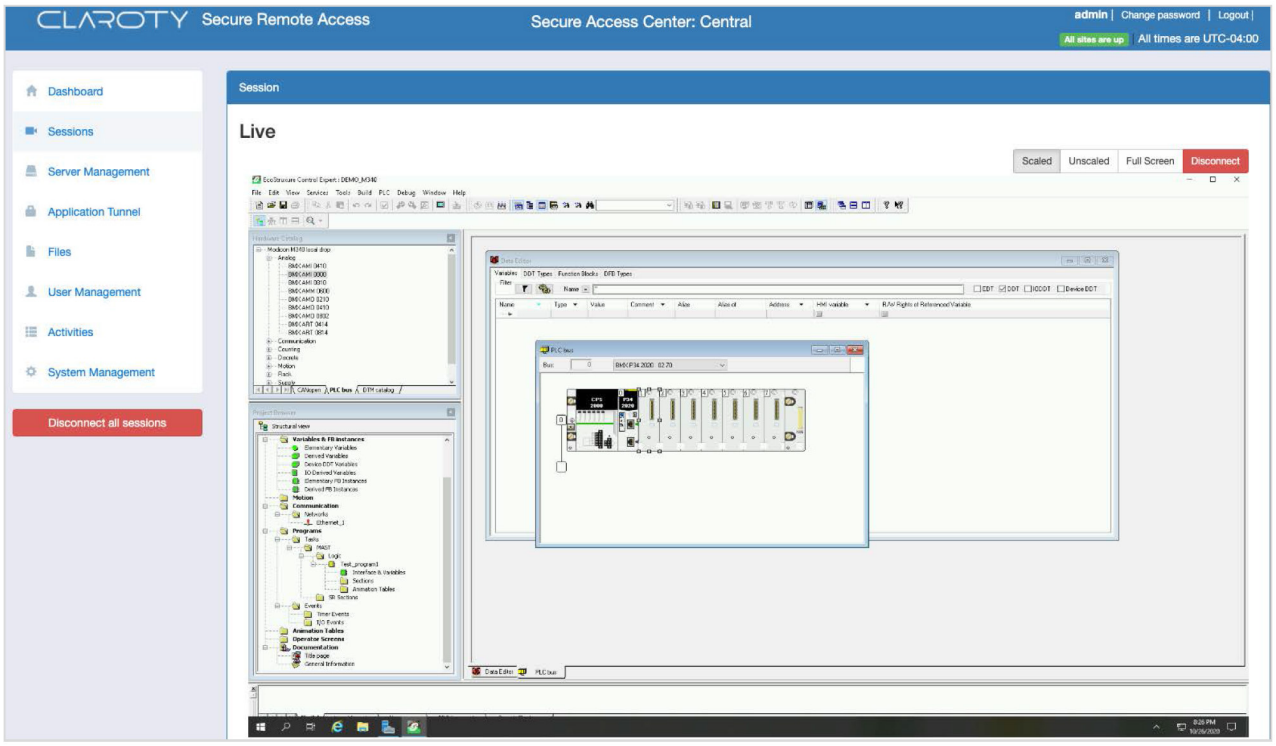

圖 5：SRA 系統管理員對使用者 SRA 遠端連線的即時全面視圖

廣泛支援遠端事件管理

SRA 可以和 Claroty 持續威脅偵測(CTD)無縫整合，讓 Claroty 平台成為業界第一個提供完全整合遠端事件管理功能的工業網路安全解決方案。

這些功能涵蓋整個事件生命週期，讓您可以從任何位置偵測、調查與回應幾乎所有可能攻擊面的工業網路安全事件。因此，您可以針對遠端、分散式及/或多變的工作環境輕鬆發展與調整貴組織的整體安全結構與工作流程。產品特性包括：

- **接收和 OT 遠端使用者活動相關的警示：**當使用者涉及未經授權或異常的活動—例如，在非預定的維護時段進行設定下載或維護資產—同時透過 SRA 連線至工業網路時，CTD 便會觸發警示。這些警示包括 SRA 使用者、工作階段的意圖、相關指標、涉及的資產，以及根本原因分析等詳細資料，可以為優先順序和分類的工作提供支援。
- **調查 OT 遠端使用者活動：**和 OT 遠端使用者活動相關的所有 CTD 警示均包含一個指向相關 SRA 工作階段的直接連結，並且具備即時監控該工作階段的能力。如果工作階段不再作用，警示將直接連結至可供調查目的檢視的完整長度視訊記錄。
- **回應 OT 遠端使用者活動：**與 OT 遠端使用者活動相關的所有 CTD 警示，也可以讓系統管理員在必要時能夠立即將相關 SRA 工作階段中斷連線做為回應動作，以防止、遏制及/或補救未經授權變更或其他 OT 遠端使用者活動所造成的任何損害。

關於 Claroty

Claroty 能夠協助組織保護工業(OT)、醫療保健(IoMT)，以及企業(IoT)環境中的網路實體系統：泛物聯網(XIoT)。公司的整合平台可以將客戶現有的基礎網路架構整合，提供可視性、風險和弱點管理、威脅偵測，以及安全遠端存取的全方位控制。

Claroty 獲得全球最大的投資公司和工業自動化供應商支援，有數百家企業組織在全球數以千計個站台部署。公司總部位於紐約，業務遍及歐洲、亞太地區和拉丁美洲。

智慧資安科技股份有限公司

服務專線　04–24523928 分機 300、301、302

電子信箱　servicedesk@unixecure.com.tw

台北據點　114 台北市內湖區基湖路 35 巷 13 號 8 樓

官方網站　facebook