CLOUDFLARE

白皮書

希望就在眼前：如何在經濟不確定時期打造更好的網路安全狀態

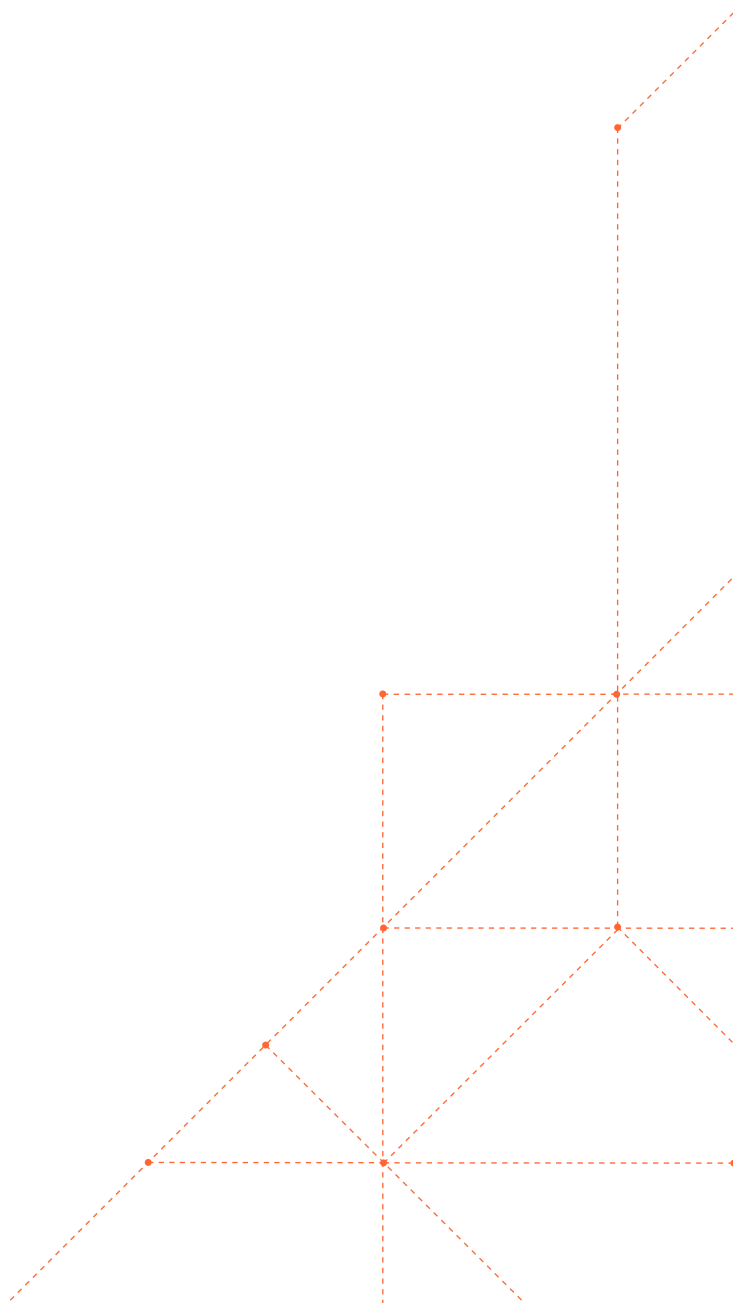
目錄

報告摘要

隨著經濟前景越來越無法預測，各組織都面臨著極大的經濟不確定性。而這種不確定性，通常表現為預算縮減，迫使資訊長和技術領導者不得不尋找新的前進道路。

幸運的是，一些領導者透過制定策略來主動調整預算、重新定義程序以提高效率，並在不大量增加資源的情況下繼續推進增長計劃，從而渡過了難關，他們在不確定性逐漸消退之後仍會處於有利地位。

在下面的章節中，我們將定義並詳細闡述造成上述情況以及市場狀況的不同因素。根據這些深入解析，我們定義了領導者可以採取的五項措施，從而尋找機會來提高安全做法效率，而不影響安全狀態。透過調整 IT 基礎架構策略來適應新的經濟環境，領導者可協助組織做好充分準備並在未來取得成功。



介紹

在過去幾年間，IT 領導者在規劃和執行策略的同時，一直在應對一場又一場危機。他們不得不對全球疫情及其連帶影響、供應鏈短缺、東歐衝突升級以及可能出現的經濟衰退做出反應。用史丹福大學經濟學家 Paul Romer 的話來說就是，「浪費危機是很糟糕的一件事 (A crisis is a terrible thing to waste)」(來源)。資訊長在支援遠端員工方面做出的選擇會產生長期的意想不到的好處，使其工作場所在支援遠端工作方面具有極大的吸引力。現在也一樣，領導者們面臨著越來越糟糕的經濟前景，他們在網路安全、網路功能、遠端存取、儲存、開發和基礎架構方面做出的選擇將助力他們保持更強勢有利的地位，從而在未來實現安全的永續增長。

遠端工作模式的興起伴隨著勒索軟體和複雜網路威脅的激增，它們為營收影響、規模和複雜度建立了新的基準 (來源)。而網路週邊剩餘部分的消失，再加上員工流動率的歷史性增長，導致網路安全漏洞出現和策略性 IT 專案延遲。這迫使組織不僅要重新思考雇用和保留員工的方法，還要重新思考控制系統和電腦存取的方法。儘管疫情導致電子犯罪率大大升高 (來源)，但也讓組織及其董事會看到了實施有效網路安全的迫切性和必要性。現在組織應該採取更具策略性的方法打一場持久戰，從而實現安全、高效且可用的混合式工作基礎架構。

為了在預算內降低業務風險並提高組織應對迫在眉睫的新興威脅的能力，您可以採取以下五項措施：

1. 稽核現有安全工具以發現重疊功能

組織可透過整合安全性廠商獲得很多好處。儘管沒有一個工具能夠成為 CISO 希望擁有的「靈丹妙藥」，但很多安全性操作員表示，他們認為公司花錢購買了太多工具，而這些工具卻未能提供最佳防禦。支援多個廠商的多個工具意味著您的員工要花費寶貴的時間來採購、實施、管理、疑難排解和支援大量未連線的系統，而不是保護基礎架構和資料。實際上，2022 年 6 月在 RSA 年度會議上進行的調查發現，「一半 (53%) 的受訪企業認為，他們浪費了 50% 以上的網路安全預算，但仍然無法補救威脅。43% 的受訪者表示，他們在威脅偵測和補救方面的頭號挑戰就是工具過多，而 10% 的組織則缺少有效的工具來補救網路安全威脅」(來源)。如果能夠僅僅消除其中一部分工具，不僅可以提高安全性，還會為員工節省寶貴的時間。

透過將投資從資本支出轉移到營運支出，您的短期現金流也會立即得到改善，而且還能避免被鎖定到阻礙業務敏捷性的多年資本投資。一種簡化方式是減少對傳統硬體的依賴。從傳統設備轉移到即服務解決方案後，即使預算縮減，亦可確保最高優先順序的計畫獲得資金。購買即服務模型也意味著，您可以從軟體本身更快的創新週期中受益，並消除頻繁修補傳統硬體帶來的無法避免的痛苦。無需進行修補和創新，您的團隊便可專注於真正有用的活動，為您的業務打造與眾不同的優勢。面對不確定性時，策略性簡化及整合能夠助您取得長期的成功。

2. 專注於資料而不僅僅是工具

領導團隊應考慮將工作重點轉移到更好的整合上，這種整合不僅局限於所有安全工具集內的工具，也包括資料，從而更好地發現模式和異常。以往，網路安全團隊隨著時間的推移，不斷增加越來越多的工具，從未考慮過在太多位置部署太多資料集的長期影響。結果通常就是拼湊了一堆產品，但幾乎毫無互通性，資料也不透明，而這會帶來發生人為錯誤的可能性，並導致洞察力更弱，準確性也更差。除此之外，團隊還需要花費時間來提取多個資料集、將其合併在一起並執行查詢，這不僅浪費了時間，也浪費了資源。取而代之的是，可以將這些資源集中於更具策略性的商業計畫上。

雖然團隊可能會找到富有創意的變通辦法來解決互通性挑戰，例如，手動合併資料集或匯入及匯出 CSV，但一定要考慮到，暫且拋開效率不談，安全工具的價值就在於這些系統處理、建立和為防禦者提供的資料。如果您的資料無處不在 —— 未分類、未受保護且管理不善 —— 則可能會讓從此類資料中衍生的原本可能有影響力的深入解析產生偏差，特別是如果影子 IT 執行個體中的資料可能會被完全忽略。透過整合工具集和周密考慮網路安全堆疊的互通性，可以降低人為錯誤，更好地保護資料。因為即使投資了目前市面上最好的工具，孤立資料集和影子資料集也會導致更差的深入解析。

就效率而言，必須考慮到，在 Zero Trust (「從不信任，始終驗證」) 時代，更多的工具意味著團隊還要花費額外的時間登入、驗證和存取系統，然後才能開始工作。任何特定員工需要接觸的系統越少，就越會節省他們的時間，讓他們能夠更快地行動。至關重要的是，要考慮到這些系統內的資料以及他們必須存取多少系統才能完成任何指定的工作，最終決定團隊能否及時應對威脅，而不是做出反應。

3. 期待即服務雲端模型最大限度實現創新並降低複雜性

每個企業都需要創新來保持競爭力，但公司若不從事網路安全業務，就沒有時間、預算或資源來跟上最新的 CVE、攻擊趨勢和重大修補，以確保整個基礎架構的安全。在可行的情況下，採用即服務模型可讓領導者從持續創新中受益，而不必擔心圍繞技術債務做出取捨或艱難的決定。

同樣還必須考慮到，一些安全服務會因為超出流量限制而收取超額費用，還有一些則會收取頻寬費用。請認真審視您的組織每月或每年支付的費用，以瞭解您支付的費用是否比您以為的要多。如果是，您可以藉此機會尋找其他不收取超額費用的解決方案，這不僅能夠幫您節省資金，還會增強對長期支出的預測能力，以便您的團隊更好地規劃未來。

採用這種性質的雲端來提供服務，您的組織也可以根據需要進行增縮，而不必承擔硬體機架的昂貴費用，以及隨之而來的生命週期管理的全部痛苦。在充滿不確定性的時代，企業必須對日新月異的市場狀況保有靈活度和靈敏度。當現金流令人擔憂時，能夠最大限度降低成本或將其完全消除就成為一項策略性優勢，無論市場狀況如何，這可能都意味著勉強生存和蓬勃發展的區別。

4. 提升員工體驗

根據《富比士》雜誌報道，「我們的調查發現，包含多個步驟的複雜登入程序讓工作者感到挫敗，這不僅浪費時間、降低效率，還促使他們放棄與工作相關的基本操作...極具諷刺意味的是，將近 40% 的工作者表示，他們會因為繁重的登入程序而拖延、委派或完全跳過設定新的工作安全應用程式。這就像用金錢能夠買到的最強、最高、最安全的門來保護您的家 —— 用雷射呼吸的龍加強防禦 —— 而晚上卻沒有上鎖。」防禦者不僅很難追蹤哪個工具擁有哪種功能，而且太多儀表板和太多的資料存放位置會為任何組織帶來重大的安全風險和可見度漏洞。那些希望提前應對網路安全威脅的公司必須考慮到，每按一下滑鼠、每一下按鍵輸入都會減少用於應對關鍵事件的寶貴時間、精力和注意力。為了打造更舒適更精簡的員工體驗，領導層一定要認真審視，防禦者有效完成工作需要使用多少種工具，以及可以消除或整合哪些工具來減少防禦者應對嚴重安全事件 (而不只是做出反應) 所需的時間。

當涉及到非技術員工或非防禦者角色的員工時，還必須考慮到，遠端工作者希望提高個人生產力時，可能會轉向影子 IT 或變通方法。儘管 Zero Trust 控制項為建立更安全的組織 (特別是在遠端環境中) 提供了一條頗有前途的道路，但不可否認，並非所有的 Zero Trust 方法都是一樣的。員工存取所需資訊越複雜，就越有可能想方設法規避而不是遵守安全控制項。領導者不僅應設法瞭解安全產品的有效性，還應考慮易用性，因為忽視員工體驗會增加整體組織風險。

5. 尋找不影響網路效能的安全服務

這不僅僅是工具的問題，如何設定和管理工具也會讓結果大不一樣。考慮讓團隊稽核目前的設定和自訂項目，以發現可能有助於增強效能的機會。如果無法提升效能，請考慮找出從頭開始專為效能而構建的解決方案 —— 因為事後改進效能很少能夠實現領導者希望達到的目標。當談到網路效能時，一定要記住，無法淘汰糟糕的架構。與地基建成後重新設計建築藍圖的機會有限一樣，網路必須從頭開始設計才能實現最佳效能。

利用全球邊緣網路在距離來源最近的地方處理資料的強大功能，將為組織的今天和未來提供策略性優勢。根據《MIT Technology Review》的報道，「處理大量資料可能會導致效能問題。因此，很多組織開始使用邊緣運算，即在距離來源較近的位置處理資料，實現了快速的即時分析和回應，同時能夠符合隱私權和安全性要求」(來源)。透過從策略上選擇基於未來架構而構建的解決方案，您可以為團隊提供網路效能更佳的策略性優勢，而不犧牲隱私權和安全性的關鍵要素。

總而言之，為了在經濟不確定時期打造更好的網路安全狀態，您可以採取以下幾項措施：

1. **稽核現有安全工具以發現重疊功能**
   - 整合重疊工具
   - 將投資從資本支出轉移至營運支出
2. **專注於資料而不僅僅是工具**
   - 工具互通性會產生更好更準確的資料集
   - 資料集和報告越準確，越會產生更好的深入解析，這對實現業務目標至關重要
3. **期待即服務雲端模型最大限度實現創新並降低複雜性**
   - 如果您不從事網路安全業務，則可以透過消除修補、維護並升級至即服務產品來獲得很多好處
   - 即服務雲端模型可提供在起伏不定的經濟環境中保有靈活度所需的彈性
4. **提升員工體驗**
   - 在太多位置部署太多工具會導致安全盲點和員工挫敗 —— 整合與簡化有助於最佳化員工體驗
   - 實現員工易用性最佳化有助於留住員工，防止他們轉向影子 IT 來完成工作
5. **在目前的網路安全堆疊中尋找隱藏的成本和效能增強機會**
   - 稽核現有工具以發現最佳化效能的機會，但請記住，無法最佳化糟糕的架構
   - 採用在全球範圍內構建且最靠近您預期客戶所在地的工具，讓您的組織提供卓越而安全的客戶體驗

Cloudflare 如何助您一臂之力

Cloudflare 成立於 2010 年，即 2008 年經濟危機結束後的那段時間，旨在引領從內部部署基礎架構向雲端轉型。我們在設計 Cloudflare 平台時懷有一個大膽的目標：助力構建更好的網際網路。Cloudflare 的產品套件可保護和加速連線至網際網路的任何事物，且無需新增硬體或安裝軟體，也不需要改動任何程式碼。由 Cloudflare 提供支援的網際網路資產透過智慧的全球網路路由傳送所有 Web 流量，每一個要求都會讓該網路變得更加智慧。我們協助客戶更智慧地工作、構建更好的產品、更快速地執行以及更安全地成長。如今，Cloudflare 可以保護並加速數百萬項網際網路資產。

控制

功能強大的整合式全球網路不僅提供全面的連線性、安全性和運算能力，還可助您實現對各種原則的控制。

靈活性

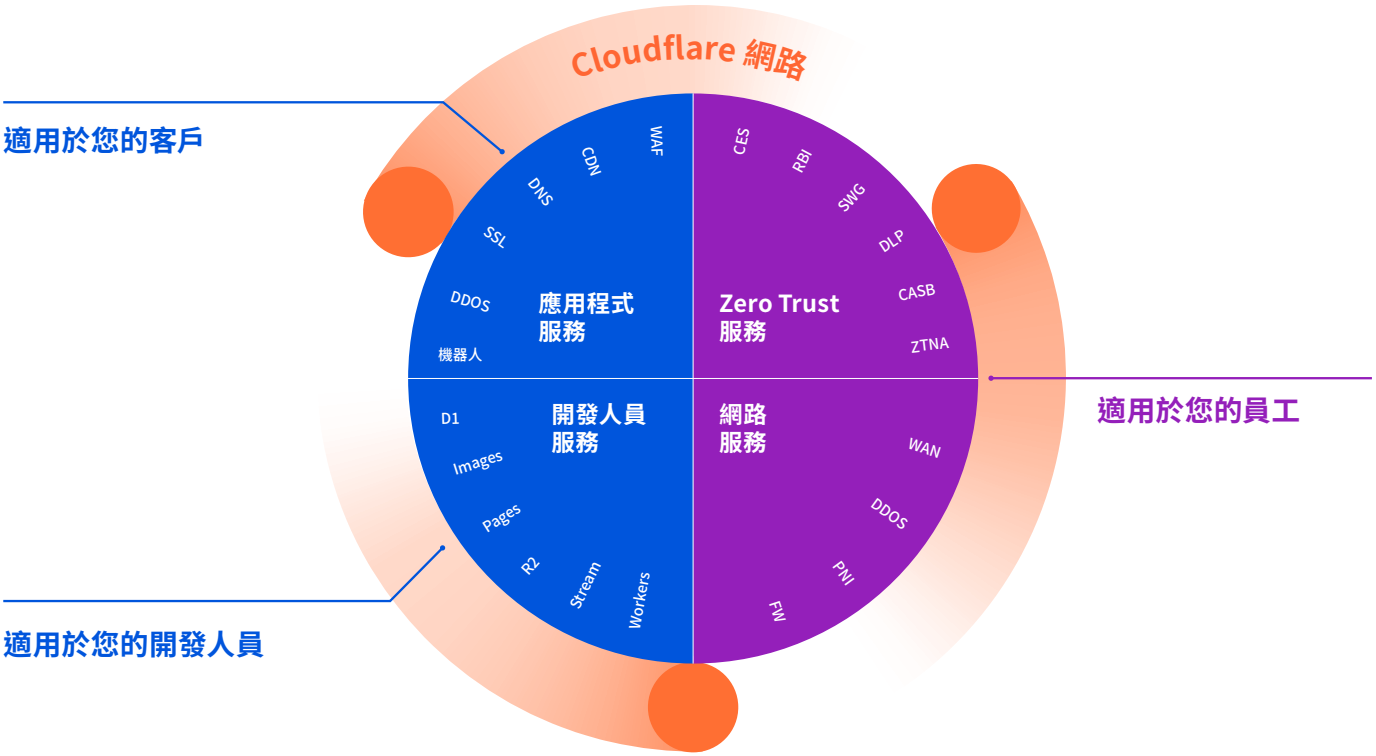
雲端原生服務意味著無需前期資本支出投資。輕鬆增減使用量以適應業務波動。

可預測性

可預測的帳單，沒有無界限輸出費用等非預期成本。無需現在為明年提供的硬體花費資本支出。

Cloudflare 全球網路可讓您連接到網際網路的一切都安全、私密、快速和可靠。

- **保護**您的網站、API 和網際網路應用程式
- **保護**企業網路、員工和裝置
- **撰寫**和**部署**在網路邊緣執行的程式碼



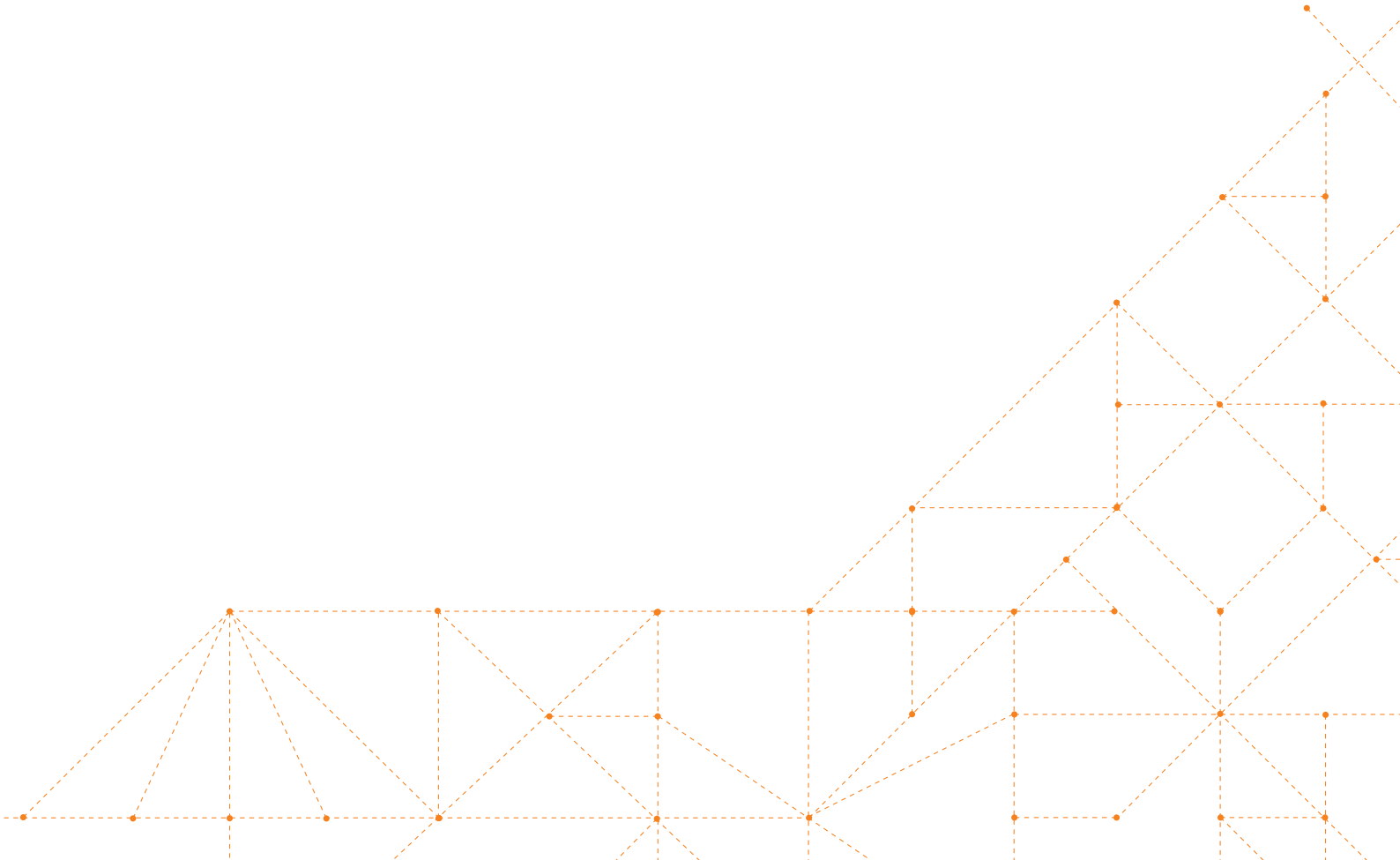
我們的平台

關於 Cloudflare

Cloudflare 成立於 2010 年，旨在引領從內部部署基礎架構向雲端轉型。我們從頭開始構建了 Cloudflare 的平台，並在其中融入了我們的大膽計畫：助力構建更好的網際網路。Cloudflare 的產品套件可保護和加速任何線上網際網路應用程式，而無需新增硬體或安裝軟體，也不需要改動任何程式碼。

由 Cloudflare 提供支援的網際網路內容透過智慧的全球網路路由傳送所有 Web 流量，每一個要求都會讓該網路變得更加智慧。我們協助客戶更智慧地工作、構建更好的產品、更快速地執行以及更安全地成長。如今，Cloudflare 可以保護並加速數百萬項網際網路資產。

若要進一步瞭解，請造訪 www.cloudflare.com



CLOUDFLARE

+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-4327.2023MAR10