zscaler™

ThreatLabz 2026: Frontier AI Readiness 報告



目錄



執行摘要 3

資料統計 5

評估群體 6

威脅展望 7

方法論 9

重點發現 10

新型攻擊鏈：
Frontier AI 如何自主地將微小缺口串聯成單一的攻擊序列 15

案例證據：
三個發展中的組織 16

實施現實性：
90 天衝刺的實際要求 18

建議 19

©2026 Zscaler, Inc. 保留所有權利。

執行摘要

去年，我們接聽到一家知名 AI 公司的來電。我們剛剛收到通知，他們發布了一款 Frontier AI 模型，該模型經過調諧，可以執行自主安全測試。那次通話啟發了我們幫助各組織做好準備，評估其應對這些自主攻擊的能力的旅程。研究結果和該模型的功能一樣令我們感到驚訝。

值得注意的是，我們並沒有將 Frontier AI 應用程式於組織的環境中；反而，我們首先在自己的基礎設施上進行測試，並利用這些深入解析開發我們現在提供的評估程序。

目的不僅在於指出缺口，還有助於說明組織在為應對新一波威脅做準備時，哪些方面可以加強安全。我們都在共同學習，這些發現不僅是為了發出警告，更是為了讓我們共同吸取教訓，從而全面提升復原力。

由於 Zscaler 採用雲端原生架構，這與大多數企業執行的混合和舊型環境不同，所以我們使用與真實模型相同的前沿測試方法，並使用類似有效率的模型和 TTP 來複製這些方法，以模擬這些敵手如何在組織的環境中運作。這使我們能夠根據企業基礎設施的運作實際情況來建置和校準評估程序，而不是根據我們自己的架構來建置和校準。

我們最大的發現：應對 AI 的致勝之道並非只是增加 AI，而是透過設計架構來杜絕可利用的弱點路徑。

全球企業尚未做好應對 Frontier AI 網路攻擊的準備，但原因並非如大多數人所設想。危險不在於 AI 會發現前所未見的奇特漏洞。前沿模型能夠利用顯而易見的漏洞（每個組織都知道存在的漏洞），並以機器速度串聯漏洞而形成完整的攻擊路徑。大多數架構的設計初衷並非如此，無論是依靠人類還是工具，試圖超越 AI 都是一場注定失敗的戰鬥。只有架構才是贏家。好消息是，只要建立正確的零信任架構，大多數企業就能比想像的更具復原力。

Frontier AI Readiness 評估計畫旨在衡量組織抵禦特定類型攻擊者的能力：這種 Frontier AI 模型以機器速度運作，並具備自主偵察、漏洞鏈結（Vulnerability Chaining）和橫向移動的能力。我們使用「Frontier AI」一詞來描述這類敵手，因為 Frontier AI 能夠以傳統掃描器甚至人類分析師都無法企及的速度，對攻擊面進行推理。在比對生產環境的平行測試中，在具有實際語境的情況下，前沿模型（Frontier Model）展現出高信雜比的推理能力，從而有效地倍增攻擊鏈發現的能力。這些能力並非紙上談兵，而是已經過證實。

©2026 Zscaler, Inc. 保留所有權利。

在 2026 年上半年評估的數百家企業組織中，包括金融服務、醫療保健、製造業、能源等八個產業的《財富》500 強企業，平均 Frontier-AI-Readiness 得分 37 分（滿分為 100）。幾乎所有組織 (91%) 擁有可公開存取的 AI 基礎設施，而且所有組織 (100%) 皆未實施基於身分識別的存取控制。此外，所有組織皆未檢查足夠的加密流量，以確保其安全堆疊能夠按設計運作。一般企業對其自身網路中傳輸的資料有 64% 的實際盲區，而且所有企業皆無法彌合擁有防禦能力與實際運用防禦能力之間的缺口。

最迫切的新缺口加劇了上述結構性發現：在所有接受評估的企業中，AI 治理都處於起步階段。包括 CoPilot、推理 API、MCP 端點和影子 AI 閘道在內的 AI 攻擊面正以遠超資安計畫吸收和治理能力的速度迅速激增。

這為提升應對 Frontier AI 威脅的準備能力提供重要契機。我們發現，近三分之一的組織可以透過將欺敵技術擴展到關鍵咽喉點來顯著提高防護能力。同樣，將入侵防護推向全面強制執行模式、整合應用層異常偵測以及改進分段政策，都是提高 SOC 警報保真度和整體防禦態勢的具體、高影響步驟。

資安領導者應該閱讀這份報告，以此作為董事會層級討論的催化劑。在 90 天內實現可以 Frontier-AI-Readiness 得分從平均 37 分提升到目標介於 73 分到 98 分之間，所有五大防禦支柱達到抵禦 Frontier AI 攻擊的有效運作臨限值。這需要三項執行措施：(1) 將 Frontier AI 復原力設立為企業命令，並向董事會匯報；(2) 確保內部高階主管達成協議，並投入專門的衝刺能力；(3) 執行雙軌衝刺，同時啟動休眠的控制措施並控制每個 AI 介面。

對所有組織而言，營運起點都相同：從現有資源著手。策略起點則是治理：任何組織都不能拖延 AI 存取安全，否則就會面臨弱點被利用的暴險。



DEEPEN DESAI
Zscaler 網路安全執行副總裁



GEORGE MOSER
Zscaler 全球副總裁兼首席體驗長



©2026 Zscaler, Inc. 保留所有權利。

資料
統計

100% 的受評估組織的 AI 缺乏基於身分識別的驗證。

91% 的組織擁有可公開存取的 AI 基礎設施，使其完全暴露在外部攻擊之下。

37 分（滿分 100 分）。最低分為 17 分，最高分為 60 分。

SSL 檢查率介於 **0.4% 至 68.1% 之間，平均約為 36%**。這遠低於 70% 檢查位準，而 70% 的檢查位準被認為是採用內嵌式安全控制（DLP、IPS、沙箱、AI 外傳）實現可接受的安全覆蓋率所必需。

在最壞情況下的爆發半徑場景中，權限最高的身分可以存取 **483,250 個應用程式**

在代表性萬用字元案例中，僅 195 個萬用網域名稱就暴露超過 **108,033** 個應用程式。（萬用字元是指使用諸如「*」之類的符號或在政策中使用前導「.」來同時表示多個網域或路徑，這提高管理效率，但如果控制不當，則會大幅擴大攻擊面。）

十個組織中 有九個都暴露了 VPN 設備。每個 VPN 設備都是預身分驗證攻擊面，可以機器速度探測 Frontier AI 模型。

750 多個資產存在 CISA《Known Exploited Vulnerabilities》（已知已被利用的漏洞），已透過主動探測來確認這些漏洞，並且在評估時這些漏洞正被主動利用。

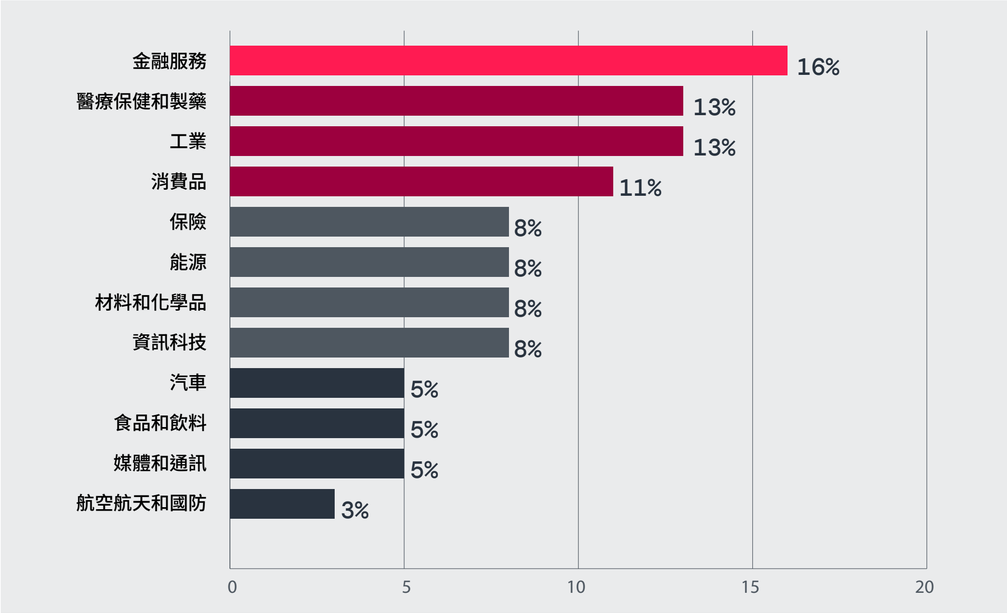


©2026 Zscaler, Inc. 保留所有權利。



評估
群體

本報告中的發現結果來自 2026 年上半年對數百家企業組織進行的 Frontier AI Readiness 評估。32% 企業是《財富》500 強企業。該群體涵蓋 12 種產業，構成如下：



接受評估的組織主要是擁有數萬個可透過網際網路發現的資產的大型企業。可透過網際網路發現的資產包括無需身分驗證即可從公共網際網路存取的任何系統、應用程式或端點。

©2026 Zscaler, Inc. 保留所有權利。



威脅展望

Frontier AI 模型已證明能夠以機器速度識別和鏈結企業漏洞。

以上結論描述當前狀況：即 2026 年上半年該群體所觀察到的情況。下文的威脅展望解釋啟動時間表的重要性。利用這些狀況的攻擊者能力發展速度遠超過企業營運週期。以下每一項趨勢都直接強化一項或多項評估結果。

在 Zscaler 的前沿模型測試計畫中，Frontier-AI 級模型在三種模式下進行評估：黑盒測試（不提供任何內部知識）、白盒測試（提供原始程式碼、經編譯二進位檔和靜態檔案）以及灰盒測試（提供部分或完整的系統語境）。這些測試獨立證實，在提供實際語境後，Frontier AI 模型能夠以高信雜比對企業環境進行推理，並持續識別出人工分析師和傳統掃描器未能發現的多步驟攻擊鏈。在生產架構中，使用實際語境已被證明能夠顯著提升攻擊路徑發現的能力。

這項獨立驗證確認，第 1 至 6 項發現中確定的組態缺口可以被自主運作的 Frontier AI 模型利用，並且當前的前沿模型可以利用在評估群體中觀察到的這些特定條件。

AI 支援的漏洞探索很可能會加速可利用的新弱點出現，直到 2027 年。

平均弱點利用時間已變為負值：即使自動部署修補程式，也可以在修補程式部署到整個企業環境之前利用漏洞。挑戰在於結構，因為利用弱點的時間表壓縮速度遠遠超過企業變更管理的適應能力。

對於 KEV 和 EPSS 得分在 1.0 或接近 1.0 的面向網際網路的資產（正如在評估群體中所確認），揭露和主動利用弱點之間的窗期已縮短至數小時。依賴標準維護窗期修補程式的組織幾乎肯定會在補救週期中面臨已知漏洞被利用的風險。

©2026 Zscaler, Inc. 保留所有權利。

未來 12 至 18 個月內，AI 攻擊面的擴張速度可能會超過治理計畫的推進速度。

AI 治理的普遍缺失反映出 AI 部署速度與資安計畫適應之間存在結構性滯後。開發團隊、SaaS 供應商和業務部門在沒有進行安全審查的情況下部署 Copilot、推理端點和 MCP 介面。根據觀察到的擴散速度，在治理真正推廣郅覆蓋到實際營運應用之前，不受監管的 AI 規模可能會翻倍。拖延的組織很可能在評估期內面臨弱點遭利用。

透過身分外洩進行橫向移動很可能成為針對零信任環境以利用弱點後攻擊為主導的技術。

意外發現表明，身分外洩是阻力最小的途徑。Frontier AI 層級的攻擊者很可能會優先考慮竊取憑證，而不是傳統的網路攻擊。收益不成比例：透過一個身分即可存取數千應用程式。工作階段永不過期且沒有裝置態勢驗證的組織幾乎肯定會成為首批攻擊目標。

加密流量盲區很可能成為 AI 驅動的資料竊取的主要資料外流通道。

Frontier AI 可以將敏感資料編碼到加密的 API 呼叫、模型互動或雲端流量。AI 工具產生看似合法的模式，再加上無法檢查的安全堆疊，就形成不可見的高頻寬資料外流通道。此弱點很可能已經被利用，且幾乎肯定會愈演愈烈。

自主弱點鏈結很可能將從初始存取到完全入侵所需的時間縮短至幾分鐘。

暴險的 VPN 設備、KEV 漏洞、萬用字元分段和休眠偵測的融合，創造 AI 敵手可能從偵察到廣泛內部存取而不會觸發任何回應的環境。資料表明，這種完整鏈目前針對大多數群體切實可行。未來 12 個月內，攻擊老手很可能就能取得具備端到端執行能力的自主工具。



©2026 Zscaler, Inc. 保留所有權利。



方法論

Frontier AI 威脅驗證

我們在受控條件下，結合企業的實際語境，利用 OpenAI GPT-5.5 和 Anthropic Claude Opus 4.8。我們使用「Frontier AI 類別」，因為具體模型的重要性不如能力臨限值重要：自主多步驟推理、工具使用、實際語境的檢索和自導弱點利用定序。當前還是未來任何達到或超過臨限值的模型都代表了此評估所衡量的敵對類別。

同時，Zscaler 採用三種模式進行內部測試前沿模型測試：黑盒測試（零內部知識）、白盒測試（原始碼、經編譯二進位檔、靜態檔案）和灰盒測試（部分或完整的系統語境）。這些測試證實，Frontier AI 模型在具有實際語境的情況下，能夠在企業環境中實現高信雜比推理。

評分框架

每個組織都根據 Frontier-AI 威脅模型進行評分，評分採用加權 100 分制，涵蓋五個防禦支柱：躲避攻擊（25 分，25%）、限制爆發半徑（25點，25%）、控管 AI 的使用（20 分，20%）、保護資料（20 分，20%）、以及欺敵和誘餌（10 分，10%）。評分同時評估了控制權歸屬和營運啟動狀態。

資料來源

評估借鑒多種類別的輸入，包括外部攻擊面管理 (EASM)、AI 驅動的漏洞優先排序、AI 特定攻擊面探索、私有存取組態審查，以及在可能的情況下，涵蓋檢查覆蓋、政策強制執行和身分驗證狀態的內嵌式遙測資料。

評估模型

基於全面的 EASM 視覺性，Opus 引擎驗證並優先處理發現結果，以使需要採取行動的已確認的可利用弱點問題浮現，平均將候選問題精簡了 84%，在最複雜的情況下精簡了 92%。還根據補救措施的投資報酬率對 CVE 進行重新評分，交叉比對發現結果與 CISA KEV ，並確定跨已驗證攻擊面的多步驟弱點利用路徑。

本次評估涵蓋（和不涵蓋）的內容

此評估旨在評估外部攻擊面暴險和資安控制組態狀態。不評估 SIEM 規則層級的 SOC 偵測效力、事件回應就緒、身分識別提供者安全態勢或端點偵測覆蓋範圍。評分反映 AI 支援的敵手在未遇到有效控制的情況下滲透、穿越和資料外流的可能性。這並不代表整體安全態勢評分。

至關重要的是，Frontier AI 層級的攻擊可以將從偵察到資料竊取的整個攻擊鏈 (Kill Chain) 壓縮到幾分鐘內，低於成熟 SOC 的回應臨限值，並且速度足夠快，可以在人為介入之前利用組態缺口。

©2026 Zscaler, Inc. 保留所有權利。

重點發現

發現 1

企業只需幾個簡單的步驟即可極致發揮其現有的 AI 防禦能力

透過切實可行的網路安全衛生措施，組織可以顯著提高其防禦能力。

啟動機會非常廣泛。64% 的組織已準備好部署經授權的欺敵平台，以增加高保真度的偵測深度。15% 的組織已準備好入侵防禦系統，可以從監控模式轉型到全面強制執行模式。18% 的身分驗證功能可以擴展到其他網站。僅透過組態最佳化，組織就能達 73 分到 98 分的目標分數（滿分 100 分）。群體的平均起始分數為 37 分，這意味著巨幅提高個別分數。

為什麼這對於應對 AI 層級的威脅至關重要：安全工具在未完全強制執行的情況下運作，對機器速度的攻擊者的抵抗力會降低。

發現 2

無論組織規模或控制廣度，所有接受評估的企業的 AI 治理都處於起步階段

這項發現具有普遍性。100% 的受評估組織缺乏基於身分識別的 AI 身分驗證，91% 的受評估組織具有公開暴險的 AI 端點。AI 治理支柱的平均得分是 2.1 分（最高分的 10.5%，滿分為 20 分）。群體中的最高評分為 3 分（滿分 20 分）。

暴險程度相當高：公共 AI 端點在整個群體中很常見，包括暴露於網際網路的的 MCP 端點和未經身分驗證的聊天機器人或 CoPilot。觀察到最嚴重的案例包括暴露於公共網際網路的嚴重等級 GenAI 閘道。

之所以有這種缺口，是因為開發團隊、業務部門和第三方供應商部署 AI 的速度超過資安計畫適應的速度。AI 治理並非未來才有的舉措。這是每個受評估組織中目前存在的、可被利用的缺口，也是成長最快的未受管理攻擊面類別。

©2025 Zscaler, Inc. 著作權所有保留所有權利。

發現 3

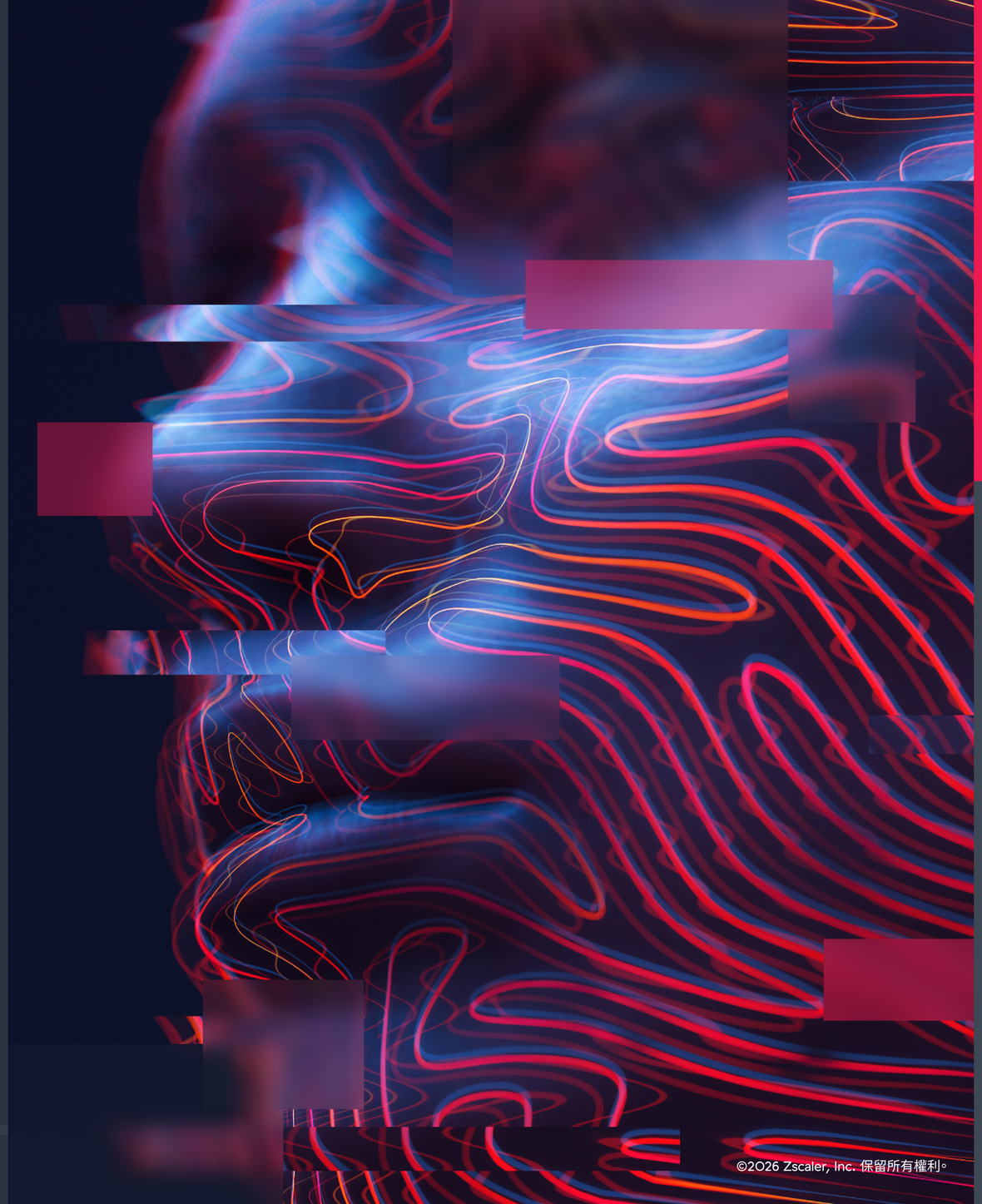
有限的加密流量檢查會降低已部署的安全控制措施對大多數流量的有效性

加密流量檢查一直是安全營運的重點工作。在 AI 威脅日益嚴峻的背景下，全面檢查覆蓋至關重要。進行資料外流的 Frontier AI 模型幾乎肯定會使用加密通道，特別是 AI API 呼叫、雲端儲存上傳以及與合法流量模式混合的模型間通訊。在未經檢查的流量中活動的敵手對內嵌式控制來說是不可見的。這使得加密流量檢查從一項操作最佳做法提升為抵禦 AI 級威脅的基礎要求。

一般企業會檢查大約 36% 的加密流量。所有組織皆未達到本評估中定義的 70% 合格檢查臨限值，即通過主動內嵌式安全控制（DLP、IPS、沙箱、AI 外傳）的加密流量比例足以使這些控制實現最佳安全覆蓋範圍。在最糟糕的情況下，99.6% 的加密流量未經過任何檢查就通過安全基礎設施。

當加密流量未經檢查時，DLP、IPS、沙箱和 AI 外傳治理等內嵌式安全控制措施將失效，導致組織對資料外流和惡意軟體傳播等關鍵威脅視而不見。鑑於超過 86% 的網路威脅和所有 AI 模型互動都使用加密通道，因此全面的流量檢查是防禦 AI 等級攻擊的必要前提。

根本原因在於營運層面，而非技術層面。絕大多數組織採用選擇加入式檢查模式（預設定為「不檢查」）。在整個群體中，組織經常依賴「繞過其他政策」或「不檢查」SSL 規則，這些規則會停用整個流量類別的檢查。在受影響的組織中，繞過規則的數量從 2 到 51 不等。



©2026 Zscaler, Inc. 保留所有權利。

發現 4

已評估的環境尚未組態成能夠以所需的速度偵測或阻止 AI 支援的攻擊

發現 4 突顯關鍵偵測缺口，因為組態（涵蓋欺敵、入侵防禦系統、異常偵測和工作階段監控）沒有針對 AI 級攻擊進行最佳化，所以啟用的安全控制措施失效，導致組織面臨他們有能力阻止但卻無法識別的威脅。因此，Frontier AI 級攻擊對 SOC 而言是不可見的，不會觸發欺敵、入侵防禦系統 (IPS)、行為異常或工作階段逾時等事件，這意味著入侵的第一個跡象很可能是外部通知，而不是內部偵測。

- **欺敵（預警系統）：**64% 的組織擁有欺敵平台，但其覆蓋範圍尚未擴展到關鍵領域。在目前組態下，橫向移動的攻擊者不會遇到任何陷阱網。欺敵系統利用高保真誘餌，觸發對橫向移動的即時自動遏制，從而提供針對 AI 驅動攻擊的有效且不依賴特徵碼的偵測。
- **入侵防禦（內嵌式攔截）：**對於 15% 的組織而言，將入侵防禦系統升級到全面強制執行模式，可以顯著加強防禦。啟用「繞過其他政策」規則後，大部分流量從未經受評估。已知利用透過加密通道傳輸將未經檢查和攔截即可通過的弱點。
- **應用層異常偵測（行為訊號）：**多個組織尚未組態內嵌式規則。萬用字元遍歷量未進行異常偵測。單一身分依序存取數千個應用程式很可能不會觸發任何警報。
- **工作階段和身分監控（遏制觸發器）：**多個組織組態的身分驗證逾時未設定過期時間，這意味著遭入侵的工作階段可能無限期地保持有效。在一個組織中，18 個存取規則均未包含裝置態勢檢查。被盜取憑證可能持續操作數週而不會觸發重新驗證。
- **對於 SOC 而言，Frontier AI 級攻擊很可能呈現以下狀態：**SOC 完全無法察覺。沒有欺敵觸發，沒有入侵防禦系統 (IPS) 警報，沒有行為異常，也沒有工作階段逾時。入侵的第一個跡象很可能是外部通知，而不是內部偵測。



©2026 Zscaler, Inc. 保留所有權利。



發現 5

廣泛的區域劃分已將私有通道平台轉變為橫向移動高速公路

我們的分析顯示，64% 使用 ZTNA 的組織存在大量使用萬用字元的組態，這可能會使比預期更多的應用程式暴險。在其中一個案例中，僅 195 個萬用網域名稱就使超過 108K 個應用程式可存取，從而可能允許單一身分在非常廣泛的環境中暢行無阻。雖然這些組態通常在部署或遷移期間引入以簡化上線流程，但隨著環境的成長，這些組態可能會一直存在，從而使存取權擴大超出最初的預期。如果沒有定期審查和改進，基於萬用字元的政策可能會削弱最小特權原則，並增加身分外洩（例如透過網路釣魚或工作階段竊取）的影響。

許多組織將身分驗證逾時設定為「永不」，這加劇了這種情況。遭入侵的工作階段將無限期地保持有效。即使是限制爆發半徑得分最高（14.4 分，滿分為 25 分）的組織，仍然保留了萬用字元組態。得分較低的組織實際上沒有進行分段。

這種模式意味著私有存取環境尚未體現零信任架構強制執行最小特權分段的設計。面對能夠大規模進行身分外洩的 Frontier-AI 級敵手，萬用字元主導組態代表了受評估環境中最具利用價值的橫向移動路徑。

©2026 Zscaler, Inc. 保留所有權利。

發現 6

超過三分之一的企業在面向網際網路的基礎設施上存在已知已被利用的漏洞。

這些風險往往持續存在，並非因為不為人知，而是因為補救措施必須與維護窗期、變更控制要求和基礎設施相依性等營運現實競爭。超過一半的群體 (53%) 收到針對網路資產的 CISA《Known Exploited Vulnerabilities》（已知已被利用的漏洞，簡稱 KEV）的修復建議。在主動探測期間，超過三分之一的企業在其邊界上維持這些可積極利用的 KEV。

結果是，防禦者補救復弱點的速度與攻擊者識別和利用弱點的速度之間日益擴大的差距。隨著攻擊者越來越多地利用 AI 來加速漏洞的探索和利用，這種暴險窗期可能會進一步壓縮。

群體中的大多數企業都出現三個 CVE。所有這些漏洞都已列入 CISA《Known Exploited Vulnerabilities》目錄。所有漏洞均透過主動探測得到確認。

- **CVE-2024-38475 (Apache mod_rewrite)：**EPSS 得分 0.9988 至 0.9997
- **CVE-2021-40438 (Apache mod_proxy SSRF)：** EPSS 得分 0.9999 至 1.0000
- **CVE-2023-44487 (HTTP/2 快速重設)：** EPSS 得分 0.999

即使在複雜的組織中，漏洞的持續存在也反映營運現實：Web 層基礎設施（特別是 Apache 和 F5/NGINX）通常不在標準自動修補程式部署範圍內，需要由人員跨變更窗期進行協調。



雖然目前暴險反映已知的漏洞，但在其邊界上存在已知 KEV 的組織也面臨風險，因為在現有補救措施完成之前，同一系統中尚未揭露的漏洞仍可能遭利用。

「發現 5」進一步加劇這種風險，因為每個未部署修補程式的面向網際網路的資產都代表身分驗證前的入口點，而且在單一身分可以存取數十萬個應用程式的環境中，被利用的 CVE 可以將存取權擴展到超越受影響的伺服器之外。

優先行動是透過外部攻擊面管理來維持持續的資產可見性，透過由代理伺服器存取來減少可發現的攻擊面，透過基於可利用性的優先排序來縮短業務合理的暴險資產的偵測–分類–修補程式部署週期，並在修復視窗期間使用自主虛擬修補程式部署。

©2026 Zscaler, Inc. 保留所有權利。

新攻擊鏈：
Frontier AI 如何自主地將小缺口鏈結成單一攻擊序列

這些發現並非個案，而且正在加強更廣泛弱點鏈中的環節。個別地，每一缺口都是可以解決的問題；但綜合起來，這些缺口造成的問題比任何一項單獨發現所顯示的都更嚴重。

具有實際語境的 Frontier AI 模型可以自主識別和定序各種條件，例如未部署修補程式的 CVE、尚未強制執行的 IPS、萬用字元組態、不受控管的 AI 端點和未經檢查的外傳路徑，從而以機器速度構建連續的利用弱點路徑，而無需人力介入。傳統掃描器和滲透測試無法以相當的速度發現這種複合路徑。已在多個評估環境中驗證以下序列：

步驟 1：透過網路掃描列舉暴險的 VPN 設備（超過 500 個設備中之一者），在 Web 層辨識出 CVE-2024-38475 (Apache mod_rewrite, EPSS 0.9997)。

步驟 2：利用預身分驗證漏洞，無需憑證即可獲得初始存取權。入侵防禦系統 (IPS) 已停用，不會產生任何警報。

步驟 3：從遭入侵的 VPN 基礎設施竊取憑證，取得唯一的有效企業身分。

步驟 4：對私有存取平台進行身分驗證。萬用字元組態允許存取超過 17,000 個應用程式。逾時設定為「永不」。不檢查裝置態勢。

步驟 5：以機器速度遍歷應用程式。路徑中無欺敵性誘餌。SOC 未收到任何警報。

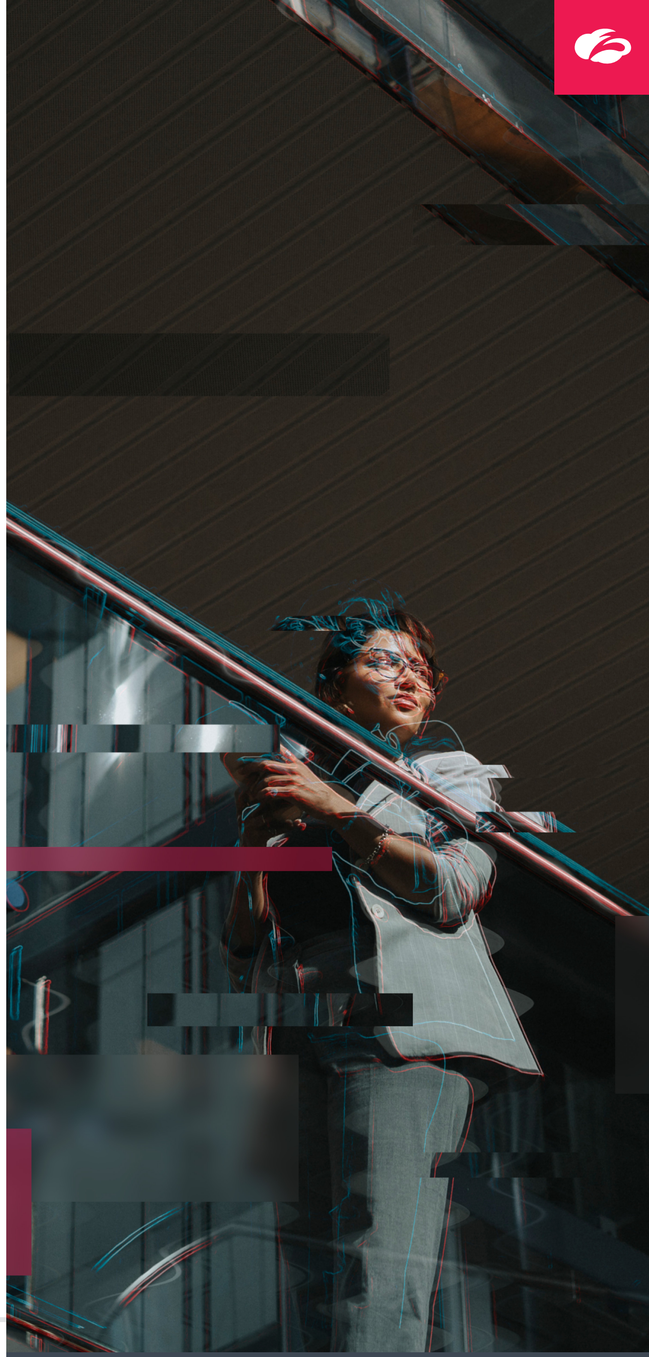
步驟 6：取得不受控管的 AI 推理端點（超過 300 個端點中之一者）的存取權，無需額外身分驗證即可存取。透過模型語境視窗查詢專有資料。

步驟 7：透過加密通道使資料外流。三分之二的流量未經檢查。資料外洩防護 (DLP) 無法偵測到外傳流量。因此不會產生警報。

從初始掃描到資料外流的總時間：在內部對抗性測試中，企業 AI 系統首次出現嚴重故障的平均時間僅為 16 分鐘。

在 Zscaler 的前沿模型測試計畫（Frontier AI 等級和 GPT 5.5，涵蓋三種模式：零內部知識、原始碼存取和部分/完成系統語境），這種推理鏈已經過驗證。這種基於實際語境的框架使前沿模型能夠識別出傳統掃描器和分析人員都無法以同等速度發現的多步驟利用弱點路徑。

在 2026 年上半年，已觀察組織環境中的每個組成部分。此鏈代表用於校準 Frontier-AI-Readiness Score 的對抗模型。



©2026 Zscaler, Inc. 保留所有權利。

案例證據：三個發展中的組織

以下匿名案例研究代表了處於不同補救階段的組織。說明初始狀態條件以及用於彌補評估過程中發現的缺口的操作方法。

案例 1

全球金融服務組織

初始狀態：超過 10,000 個面向網際網路的資產。超過 4,000 個已驗證的 CVE（超過 900 個獨特的 CVE，其中 165 個為嚴重 CVE）。在暴險的基礎設施上已確認了該群體中最常見的三個 CVE（CVE-2024-38475、CVE-2021-40438 和 CVE-2023-44487）。

評估結果：該組織的龐大面向網際網路的系統存在大量未部署修補程式的關鍵漏洞，這些漏洞是在多代基礎設施迭代中所累積。SSL 檢查尚未涵蓋大部分流量。欺敵技術已獲批准，但尚未部署。AI 應用程式仍處於治理邊界之外。

已起始補救措施：優先部署 165 個關鍵 CVE 漏洞的修補程式。SSL 檢查由選擇加入轉換為選擇退出。在核心金融業啟用欺敵攻擊防護。已啟動 AI 攻擊面閘控機制。



©2026 Zscaler, Inc. 保留所有權利。



案例2

全球食品生產商

初始狀態：13 台 VPN 設備暴險。40 個公共 AI 介面位於治理邊界之外（在所有暴險設備中，AI 暴險密度最高）。已驗證 2 個 CVE 漏洞，這些漏洞與暴險的基礎設施相關。

評估結果：該組織的快速數位轉型速度超過安全計畫整合新安全面的能力。各業務部門已將 AI 端點作為營運計畫的一部分進行佈建，但尚未將其納入安全架構。私有存取環境尚未制定分段政策。VPN 基礎設施仍面向網際網路，等待遷移完成。

已起始補救措施：立即啟用私有存取後的 VPN 保護。對 40 個端點進行 AI 攻擊面閘控。從零開始建立分段政策。在生產環境中部署欺敵技術。

案例3

全球奢侈品企業集團

初始狀態：範圍內有 487 個面向公眾的名稱。每月未經檢查的加密流量為 922 TB。有 10,000 個已定義的應用程式。

評估結果：組織的檢查架構採用保守的選擇加入模式，導致大部分加密流量未經檢查。由於擁有 10,000 個應用程式且幾乎沒有進行任何分段，環境在沒有對應存取權控管的情況下擴張規模。

已起始補救措施：SSL 檢查轉換是首要任務。在 10,000 個應用程式中替換萬用字元。啟用欺敵機制。建立 AI 治理基線。

©2026 Zscaler, Inc. 保留所有權利。

實施現實性：
90 天衝刺的實際要求

技術上，在 90 天內實現復原力切實可行，因為大多數情況下，控制措施已經到位，也充分理解相依性鏈。然而，由於這並非易事，因此需要行政部門的強制命令。彌合 Frontier AI Readiness 差距是一項企業舉措，需要董事會層面的關注、首席資訊安全長與執行長的協調一致以及專門的執行能力。這是在不斷變化的安全威脅情況下達成共識的機會。資安領導者應該：

1. 向董事會簡要介紹目前的準備態勢，並在美國證券交易委員會 (SEC)、美國國防部監管局 (DORA) 和美國國家資訊系統監管局 (NIS2) 的監管情景下建立框架。

2. 爭取高階主管支持，展開為期 90 天的衝刺專案，明確專案負責人，並定期向高階主管報告。

3. 分配小型專門團隊執行實施工作，預期由於擴大檢查範圍、萬用字元替換期間的存取改進等原因而遇到的摩擦，是啟動流程中可預期的部分。

SSL 檢查需要跨部門協作。企業應與 IT 和資安團隊協調合作，全面瞭解當前的檢查覆蓋範圍，確定哪些流量需要檢查，並判斷哪些情況下檢查在操作上不可行（例如，憑證綁定應用程式或舊型整合）。在無法進行檢查的情況下，諸如瀏覽器隔離、端點資料外洩防護 (DLP)、CASB 的 API 檢查和 DNS 層篩選等緩解措施，可以在無需內嵌式解密的情況下，提供補償性的可見性和威脅防禦能力。

萬用字元替換需要應用程式擁有者的協調。將 200 多個萬用字元替換為具名的 FQDN（完全合格網域名稱）並非資安團隊單方面就能完成的任務。每個萬用字元都指向業務部門、開發團隊和供應商擁有的應用程式，必須驗證存取的連續性。資安團隊負責定義目標架構，但執行過程需要跨部門協作。

此時間表假設擁有專門的執行能力。已指定衝刺團隊（2 至 4 名工程師）的組織按時程推進。在現有工作負載內進行改進的組織則受益於額外的支援，從而保持進度。任務成功取決於高階主管的支持，包括定期與高階主管溝通、配備專職團隊和保障執行能力，以及每週根據目標分數提交里程碑報告。

雖然任何重大的安全更新都可能導致暫時的營運變化，但這些步驟對於建立更具復原力的長期防禦至關重要。我們的評估強調，主動解決差距（例如初始得分 37 分）是應對現代數位威脅的關鍵步驟。在進行這些短期調整的同時，也要兼顧強而有力的保護，這就是加強組織整體安全態勢的關鍵。



©2026 Zscaler, Inc. 保留所有權利。

建議

1 啟用安全控制的強制執行模式

每個受評估的組織都擁有高影響力的控制措施（IPS、身分驗證、惡意 IP 封鎖、網域偽裝保護），這些措施可以透過組態變更來全面實施。資安維運團隊應稽核所有已擁有功能的啟動狀態，酌情利用供應商組態稽核和啟動支援，並在 14 天的衝刺週期內以強制模式啟用這些功能。

我們理解每個 SOC 團隊的擔憂：將 IPS 從監控改為攔截可能會產生誤報並擾亂流量。正確的方法是漸進式部署（Phased Rollout）：先在非關鍵領域進行調整和驗證，然後擴展到生產環境，並制定明確的回溯標準。

2 立即對所有 AI 攻擊面啟用身分感知存取控制

所有可透過公共網際網路存取的 AI 端點都必須受到企業身分驗證保護。建議所有受評估機構都採取此措施。在身分感知存取實現之前，任何連網的攻擊者都可能利用 AI 基礎設施。

3 90天內將 SSL/TLS 檢查增加至少 70% 的合格覆蓋率。

將模型從選擇加入轉變為選擇退出：依據預設檢查所有流量，然後建立範圍較小的排除項。取消「繞過其他政策」規則。將「不予檢查」例外情況減少到最低限度。預計會有 2 到 4 週的應用程式中斷。指派服務台應變增援容量。如果沒有這種保護，DLP、IPS、沙箱和 AI 外傳控制將無法對大多數流量起效用。

SSL 檢查應該基於風險，而不是一概而論。先從最關鍵的應用程式和風險最高的流量入手，然後選擇性地擴展。由於某些應用程式和服務需要例外情況，例如憑證綁定或由於監管約束，組織應提前定義例外路徑和快速回應程序。在無法進行檢查的情況下，透過補償控制措施來減少可視性缺口。

4 在關鍵網段中，將萬用網域名稱替換為具名的 FQDN。

稽核所有私人存取組態中的萬用字元項目。優先更換核心系統：財務系統、智慧財產權庫、身分識別基礎設施。實施身分驗證逾時、對每個存取規則進行裝置態勢驗證，以及應用程式層級分段，將每個身分限制為僅能存取所需應用程式。制定與應用程式擁有者進行跨職能協調的計畫。



©2026 Zscaler, Inc. 保留所有權利。

5 在關鍵網路網段部署欺敵技術

組織可以在核心應用程式附近放置誘餌、建立獨立的偵測層、提供高保真警報來幫助 SOC 團隊更快做出回應，實現加強防禦。當誘餌被觸發時，欺敵技術會自動透過 ZPA 撤銷遭入侵使用者對每個已登入裝置上私有應用程式的存取權，而無需分析師批准。以此方式在攻擊者轉移之前將其攔截，阻止橫向移動的速度與攻擊的速度相同，而不受 SOC 處理排程速度限制。

6 將暴露於網際網路的 VPN 設備移至零信任代理存取之後

每個可被發現的 VPN 設備都是預身分驗證攻擊面。30 天內完成所有 VPN 基礎設施的代理存取。在 90 天內退役暴險的設備。這就消除了 Frontier AI 模型首先會探測的入口點。

7 在評估後 72 小時內部署面向網際網路資產上 CISA-KEV 漏洞的修補程式

CVE-2024-38475、CVE-2021-40438 和 CVE-2023-44487 的 EPSS 得分接近或等於 1.0，並且已確認有活躍的弱點利用。立即進行修補程式部署或虛擬修補程式部署。在需要維護窗期的情況下，部署自主虛擬修補程式來阻止在此期間的攻擊嘗試。



©2026 Zscaler, Inc. 保留所有權利。

監管
暴險說明

得分低於 40 分的組織可能存在控制弱點，這會增加發生重大網路安全事件的可能性和潛在影響。我們鼓勵各組織審視本報告中的建議並採取行動，以協助降低風險暴露並增強抵禦能力。在某些情況下，根據美國證券交易委員會第 1.05 項（8-K 表格），與這些弱點相關的事件也可能引起揭露考慮。

對於受 DORA 或 NIS2 監管的組織而言，基礎控制的缺失也可能意味著有機會加強 ICT 風險管理和整體營運復原力。

後續
步驟

Frontier-AI-Readiness 評估為每個組織提供量化的初始分數、優先的補救順序以及 90 天可達成的目標，主要透過擴展或微調現有能力來達成目標。本報告中的資料確立產業基準。對於每一位資安領導者，關鍵問題是：他們的組織相對於 Frontier-AI-Readiness 處於什麼位置？

您已經看到發現結果。現在瞭解您的暴險。

與 Zscaler 專家交流，確定您的環境中可能存在的 AI 風險以及首先需要解決的問題。

瞭解風險，快速應對，持續守護安全。
瞭解更多資訊，zscaler.com/campaign/zscaler-ai-security-demo

關於
ThreatLabz

ThreatLabz 是 Zscaler 的安全研究部門。這支世界一流的團隊負責搜尋新型威脅，並確保使用 Zscaler 全球平台的數千個組織始終受到保護。除了惡意程式研究和行為分析之外，團隊成員還參與 Zscaler 平台上進階威脅防護新原型模組的研發，並定期進行內部資安稽核，以確保 Zscaler 產品和基礎設施符合資安合規標準。ThreatLabz 定期在 research.zscaler.com 發布新興威脅的深入分析報告。

關注我們：X @ThreatLabz | ThreatLabz 安全研究部落格

©2026 Zscaler, Inc. 保留所有權利。

zscaler™ | 快速應對。持續守護安全。

關於 Zscaler

Zscaler（NASDAQ：ZS）致力於加速數位轉型，使客戶能夠變得更敏捷、更高效、更具有復原力且更安全可靠。 透過安全連接處於任何位置的使用者、裝置和應用程序，Zscaler Zero Trust Exchange™ 平台可保護數千名客戶免受網路攻擊和資料遺失的侵害。基於 SSE 的 Zero Trust Exchange™ 平台分佈在全球 150 多個資料中心，是全球最大的線上雲端安全平台。造訪 **zscaler.com** 了解更多資訊；或在 Twitter 上關注我們：**@zscaler**。

© 2026 Zscaler, Inc. 保留所有權利。Zscaler™ 及其它商標，均列於 **zscaler.com/legal/trademarks** 是 (i) 在美國註冊的商標或服務標誌，或是 (ii) Zscaler, Inc. 在美國和/或其它國家的商標或服務標誌。其它所有商標，均為其各自所有者的財產。

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**