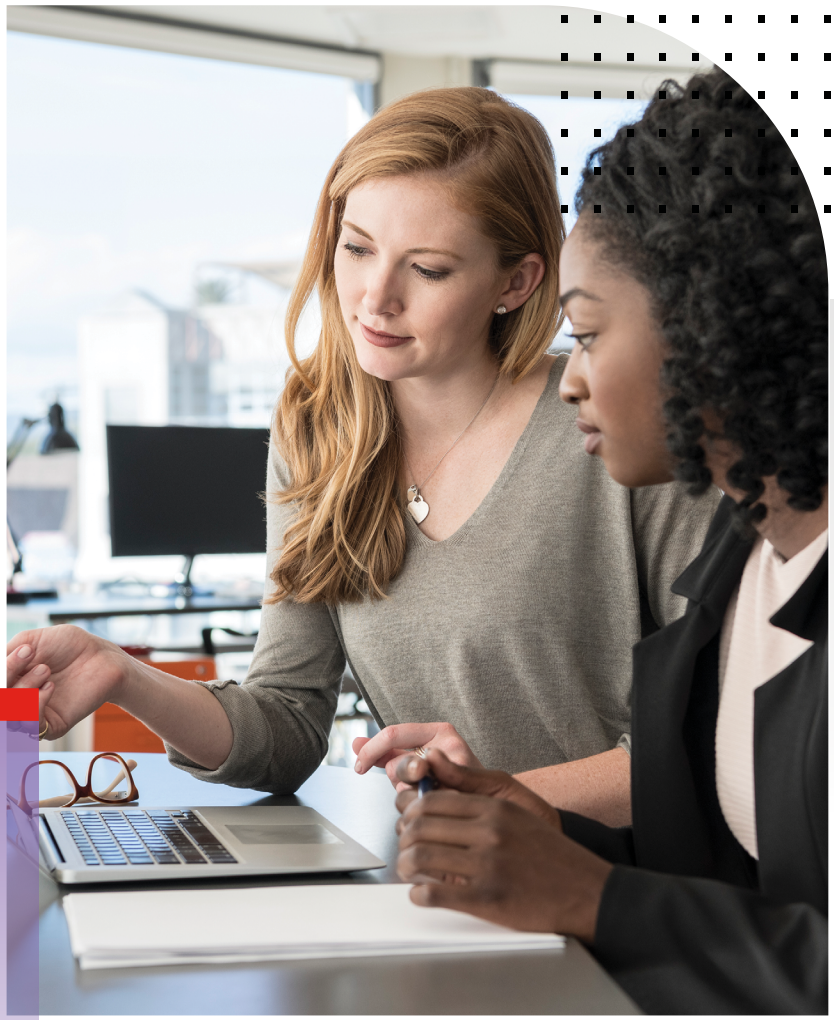
白皮書

防護數位創新需要零信任存取

隨著攻擊面擴大，企業資安長們將面臨新的風險



內容摘要

為了加快業務發展並保持競爭力，許多企業正迅速採用數位創新 (DI) 計劃。這意味著企業裏的許多業務與資料分散在遠離公司本身很遠的地方，使員工可以從許多地方存取更多的公司資源。出於這個原因，傳統的邊界概念正在瓦解，這使得內部網路面臨不斷擴大的攻擊面，而這也是許多企業資安長們最關心的議題。

為了應對這些威脅，企業組織需要採取“不信任任何人，不信任任何人”的安全方法。具體來說，資安長需要使用零信任存取 (zero-trust access，ZTA) 策略來保護網路，確保雲端中的所有用戶、所有設備和所有 web 應用程式都是可信且經過身份驗證的，並且具有正確的訪問量。無論單個項目的性質如何，零信任對於確保數位創新至關重要。

有 81% 的企業領導人表示，員工現在是行動網路安全的最大風險。[1]

網路邊緣環境的進化

對於各種規模的企業，數位創新 (DI) 計劃可推動業務成長。這種成長的一個方面是新網路邊緣設備的激增，比如：私有和公共雲端基礎架構、物聯網 (IoT) 和行動設備、軟體定義 (SD) 分支架構的產生等等，所有這些都產生倍數成長的資料、應用程式和工作流程。為了管理用戶訪問並將來自不同地點的一系列設備在網路上和網路外互連，許多企業組織正在增加部署在這些網路邊緣的設備數量。

對於資安長來說，這可能是一場噩夢。近年來，網路邊緣設備爆炸式成長，以至於傳統的邊界概念正在瓦解，並創造了一個適合攻擊的開放環境。網路威脅正變得越來越多產且不斷變化。過去，週邊安全是基於“信任但核實”的方法。但是由於網路上有這麼多的用戶、設備和應用程式，很難知道該信任哪些用戶、設備和應用程式。諸如憑證盜竊和惡意軟體之類的漏洞攻擊可以讓駭客獲得合法帳戶的存取權限。而一旦進入，這些不良行為者很容易找到橫向移動的方法，迅速擴散並利用扁平而可信的內部網路。一旦獲得邊緣設備的存取權限，滲透者就可以發起攻擊，從而導致營運停機、資料被盜、財務損失和聲譽損害。

對於資安部門負責人來說，使用傳統的網路存取方法無法跟上越來越多的入侵與攻擊。這就是為什麼發生從信任網路上的一切到變成不信任一切。透過一個運作良好的零信任存取模型，資安長依照網路邊緣的特定脆弱區域來分類，這些區域被認為是不可信任，分別是：用戶、設備和網路內外的資產。

知道 *誰* 在連接網路

資安部門負責人需要始終知道誰在網路上。然而，當涉及到使用弱密碼連接到網路的員工時，企業面臨的風險就會增加。因為現在有這麼多帳戶需要密碼登入，所以許多密碼設定過於簡單，很容易遭受網路釣魚攻擊等漏洞而被洩露攻破。對於企業來說，了解每個用戶以及他們在公司中扮演的角色至關重要。只有掌握了這些知識，他們才能安全授予對每個角色或工作所需的資源存取權限，同時根據具體情況向其他人提供額外的存取權限。

雖然自帶設備 (BYOD) 可能很受用戶與管理人員的歡迎，但一些資安長卻忽視了其中危險。廣泛的攻擊面使不斷演進的威脅更容易穿透傳統的外圍防禦並在內部網路橫向行動，這是漏洞可以長時間未被發現的方式之一。一些最具破壞的入侵行為是通過未經授權的用戶存取網路或透過給予信任用戶不適當的訪問級別而發生的。BYOD 在企業中無處不在，有 83% 的資安部門負責人表示，他們的企業正面臨著來自各式行動設備的威脅。[2]

企業面臨的另一個挑戰是分佈在各地工作的員工，員工在不同的地點進行工作，從公司總部到分支機構，以及越來越多的居家辦公。由於有如此多的用戶可以遠端存取網路，因此攻擊面有更多的成長機會。例如：員工們經常在咖啡店、機場、

汽車或公共交通工具上使用熱點或公共 Wi-Fi 來連接網路。這類型的連接會帶來重大的資安風險，第三方可以竊聽在用戶與公司網路之間傳遞的所有資訊。駭客可以利用未修補的軟體漏洞將惡意程式碼注入端點設備，這不僅可以存取本地資訊，還可以透過端點設備存取公司網路。

這些挑戰在大多數遠端作業環境中變得尤其突出，這是所有企業在 2020 年 COVID-19 大流行間所吸取的教訓。大多數原本計畫不到 15% 的員工來進行遠端辦公的企業，突然不得不確保他們需要擁有 90% 或更多的資安架構的需求。

這些需求是零信任存取如此重要的部分原因。由於越來越多不同設備不斷連接網路，因此確保資安部門負責人可以知道哪些用戶在網路上以及他們具有正確的存取層級非常重要。隨著員工角色的變化，例如：從業務人員轉為營運，工作人員可能不需要存取他們之前角色所擁有的相同區域，資安團隊應該能夠為相關人員實現無縫過渡。

近年來，許多組織遭遇的最具破壞性和最成功的攻擊都集中在邊緣網路設備上。[3]

知道 *什麼* 連接到網路上

除了知道誰在網路上，資安部門負責人還需要隨時了解網路上有哪些設備。然而，行動設備和物聯網產品的激增已將傳統網路邊界分解為許多微邊界，這導致企業面臨更大的攻擊面。由於每個微邊界都與每個用戶設備相關聯，因此端點設備常被鎖定成為惡意軟體感染和複雜漏洞利用的主要目標。

由於端點設備爆炸式成長和攻擊面不斷擴大，許多企業從根本上失去了對網路的控制，因為他們不再確定哪些設備正在連接到網路。事實上，BYOD 或 IoT 的配置幾乎沒有標準化。關於 BYOD，行動設備可能會使網路面臨巨大風險。這可能是由於資料洩露、不安全 Wi-Fi 連線、網路詐騙、網路釣魚、間諜軟體、密碼被破解或不正確的 Session 處理。然而，端點設備攻擊面的最大成長領域是來自 IoT 設備的爆炸式成長。

隨著企業連接越來越多的“智慧型”設備，對物聯網設備的網路攻擊正不斷發展。駭客正在利用這些設備進行分散式阻斷服務攻擊 (DDoS) 以及許多其他類型的惡意入侵。

為了完全防護 BYOD 和 IoT 端點設備，企業必須了解每個設備的位置、功能以及它如何透過網路拓撲連接到其他設備。缺乏可見性使企業容易受到看不見的風險影響。資安部門負責人必須能夠追踪網路邊緣的設備。然而，近一半的資安專業人士表示，他們沒有制定應對物聯網設備攻擊的計劃，儘管有九成的人表示對未來的威脅擔心。[4]

一些企業使用傳統的網路分段模式，但網路安全分段很難定義，有時造成有些分段可以讓被授權用戶與應用程式存取，而其他人無法存取，即使是最努力的分段，也會在網路防禦中留下漏洞 (網路架構師沒有設想到的情境)，惡意行為者可以利用這些漏洞。

此外，如果訪問權限是基於對經過審查的設備的假定信任，那麼企業仍會受到攻擊。許多企業對來自以前曾信任的員工和承包商的攻擊感到驚訝。丟失或被盜的設備可能會洩露密碼，從而使未來的網路攻擊成為可能。這就是零信任方法如此重要的原因。由於網路駭客專注於破壞廣泛的網路設備，資安部門負責人需要更好地了解和檢測連接到網路的每個特定設備。

防護網路內外的資產

資安部門負責人面臨的另一個重大問題是越來越多員工會離線或使用其他網路上的行動設備，這會在這些設備重新登入到公司網路時帶來資安威脅，例如：許多員工將 BYOD 設備用於個人和其它需求。他們瀏覽網路，在社交媒體上與他人互動，

甚至在未登錄公司網路時接收個人電子郵件。但是，當他們上線後重新登入公司網路時，員工們可能會無意中將他們的設備和公司資源暴露在威脅之下，如：病毒、惡意軟體和其他利用漏洞的攻擊，如：惡意軟體或僵屍網路。

這種個人和企業設備混合的使用方式，也是在大多數企業無法跟上網路上和網路下的端點數量的時候出現的。在 Ponemon 研究所最近的一份報告中，63% 的公司表示他們無法監控離網的終端設備，超過一半的公司無法確定端點設備的合規狀態。[5] 連接到網路的設備數量之多，掩蓋了所有端點設備的可見性。因此，資安長和資安團隊很難管理所產生的大量風險。

透過過渡到識別、分段和持續監控所有設備的 ZTA 架構，企業可以替換高風險的扁平網路，以確保內部資源保持安全，資料、應用程式和知識財產權持續受到保護。該策略不僅降低以周邊設備為中心的安全策略相關風險，而且還提高了離網設備的可見性和控制力，同時簡化了整體網路和安全管理。

有 63% 的企業無法監控離開企業網路的端點設備，53% 的企業顯示惡意軟體感染的端點設備在過去 12 個月中有所增加。[6]

結論：零信任存取方法是必需

DI 計劃可加速業務擴展。它們還給組織的資安長、他們的團隊和他們的資源增加了壓力，因為 DI 計劃可以擴大和改變企業的被攻擊面，為網路威脅開闢了新的攻擊媒介。駭客入侵變得更加複雜和先進，傳統的周邊防御方法已不再適用。根據威脅的性質和複雜度，企業的安全基礎架構中沒有任何一點可以看到威脅的所有方面。企業的安全基礎架構無法從單一個點可以看到威脅的全部面向。有了零信任存取，資安長就可以關注連接到網路的用戶與設備，確認他們的身份並確保他們擁有正確的存取和信任。

攻擊面的不斷擴大主要原因之一是物聯網和智慧型裝置的增加。資安部門負責人往往缺乏對大量接入網路設備的全面瞭解，資安長已經從他們看不到的東西中吸取了慘痛教訓。為了完全保護所有這些端點設備，企業需要在整個網路中採取零信任存取策略，該策略可提供對每個設備所在位置、作用以及如何透過網路連接到其他設備的可見性，以及持續監控檢測任何可能存在威脅的異常行為。

[1] "Mobile Security Index 2019," Verizon, 2019.

[2] Ibid.

[3] Neil Jenkins and Natasha Cohen, "Living on the Edge," Cyber Threat Alliance, April 30, 2019.

[4] "Only 47% of cybersecurity pros are prepared to deal with attacks on their IoT devices," Help Net Security, November 8, 2019.

[5] "The Cost of Insecure Endpoints," Ponemon Institute, 2020.

[6] Ibid.

FORTINET

www.fortinet.com

August 16, 2021 3:58 PM
123456-0-0-EN