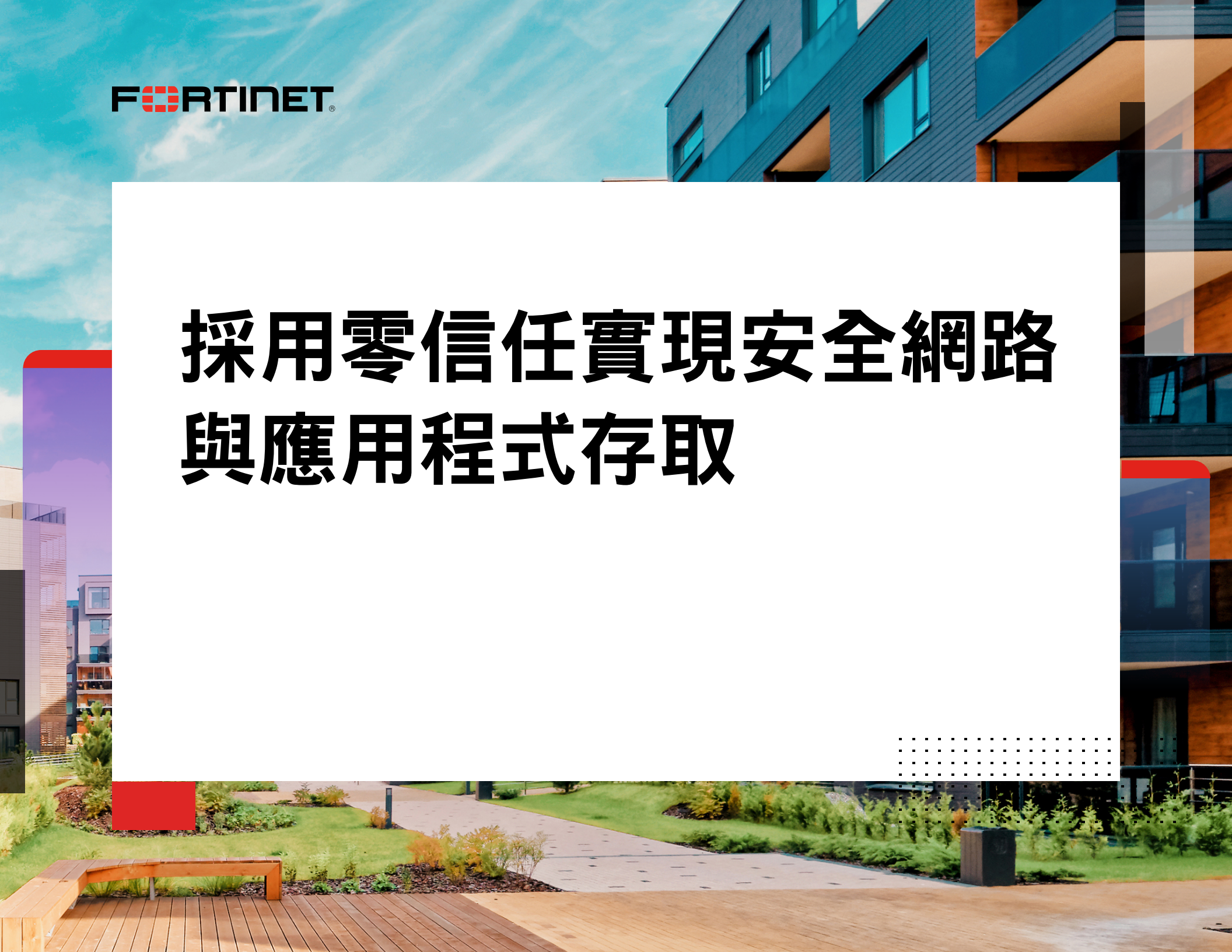

採用零信任實現安全網路與應用程式存取

目錄

概述

隨著企業不斷擁抱數字創新、雲端應用和無處不在的工作，網路變得越來越複雜和分散，“邊緣設備”的數量也越來越多。隨著傳統的網路邊界的不斷消失，連接到網路的人和設備越多，以前傳統的安全方法就越不安全。

每當一個設備或用戶被自動信任時，就會使一個組織的數據、應用和知識財產面臨風險。 資安長們需要將原本的信任授權模式轉變為零信任模式。這種零信任策略需要納入嚴格的存取控制，跨越分佈式網路，使設備、用戶、終端、雲環境、軟體即服務 (SaaS) 和基礎設施都得以得到保護。

Fortinet 的零信任存取 (ZTA) 架構使用一個緊密整合的解決方案，幫助企業識別和分類所有尋求網路和應用訪問的用戶與設備。

引言

隨著越來越多的公司轉變其網路以適應遠端工作人員、多雲架構與數位創新，他們的安全方法也需要改變。今天，企業需要從任何地方建立安全和值得信賴的存取與授權，以獲得各種基於雲端的服務與企業資源。

傳統的安全模式的假設，是在一個組織的網路內的任何東西都應該被信任。但是，自動將這種信任機制擴大到任何設備或用戶，無論是有意還是無意，都會使組織面臨巨大風險。

自帶設備 (BYOD) 和物聯網 (IoT) 計劃的增加導致各式接入點和端點設備的激增，因此傳統的網路邊界已被消除。繞過邊緣安全檢查點的攻擊者、惡意軟件和受感染的設備往往可以自由進入網路內部。

這種 ZTA 方法將固有信任開放網路轉變成零信任架構策略。該策略採用嚴格的網路存取來識別、驗證和監控網路內外的用戶與設備。

PCI DSS 遠端工作指南：要求擁有存取持卡人資料的同仁必須透過 VPN 進行並使用多因素身份驗證。[1]

有效ZTA的關鍵

今天的網路有巨大的、動態的，在某些情況下甚至是臨時的邊緣環境。許多設備經常處於離線狀態，這使得持續風險評估和授權信任變得更加困難。因為沒有辦法驗證網路上或網路外的用戶或設備是否可以信任，因此資安負責人應該假設網路上的每個設備都可能受到感染。此外，任何用戶都可能有意或無意地損害關鍵資源。

一個有效的 ZTA 策略可以解決網路連接和應用存取的問題，其基本假設是沒有用戶或設備是可信的。如果不先驗證用戶與設備是否被授權訪問，就不會對任何交易給予信任。實施 ZTA 模型需要關注三個關鍵因素。

1. 了解網路上的每台設備

由於應用和設備的增加導致網路周邊的擴大，現在必須管理和保護潛在的數十億個邊緣周邊。這方面，網路存取控制 (NAC) 工具則提供了對網路環境的可見性。

2. 了解存取網路的每個用戶

要制定有效的 ZTA 策略，確定每個用戶是誰以及他們在企業中扮演的角色非常重要。零信任模型側重於 “最低存取策略”，該策略僅授予用戶對其角色或工作所需資源的存取權限。

3. 了解如何保護網路內外的資產

有效的 ZTA 策略通過提高端點的可見性來應對保護網路外設備的挑戰。由於移動性和遠端工作的增加，用戶可能會無意中將他們的設備和公司資源暴露在威脅之下。在其他地方連線後，一旦他們重新加入網路，這些用戶可能會無意中將公司資源暴露給他們可能已經感染的病毒和惡意軟體中。

針對端點的攻擊頻率不斷增加，檢測越發不易。有 68% 的受訪者表示，在過去的 12 個月中，攻擊的頻率有所增加。[2]

Fortinet 零信任解決方案

為了實現 ZTA，Fortinet 緊密整合一系列安全解決方案，幫助企業識別和分類所有尋求網路存取的用戶與設備。不僅可以評估他們對內部安全規範的遵守況狀，自動將它們分配到相關的控制區，只要設備受管，還可在網路內外持續監控它們。此外，Fortinet 還提供傳統的零信任存取可擴展到常用應用程式的監控，因此系統管理員不僅知道誰在網路上，甚至可以得知他們目前正在使用哪些應用程式，讓使用者的任務和使用情況不斷被監控和檢查。

1. Endpoint Access Control 端點存取控制

端點往往是最早被破壞或攻擊的目標。事實上，最近的一項研究發現，有 30% 的入侵事件涉及安裝在端點上的惡意軟體。[3] Fortinet 透過整合的可視性、控制和主動防禦來加強端點安全。發現、監控和評估端點風險的能力有助於確保端點的合規性，減輕風險，並減少暴露。Fortinet FortiClient 端點存取解決方案：

- 支援跨越不安全網路的安全加密連接，支援分離式隧道和安全存取服務前端 (SASE) 服務
- 提供持續的端點安全遙測數據偵測，包括設備作業系統 (OS) 和應用程式、已知的漏洞、補丁和安全狀態

2. Identity Access Management 身份存取管理

今天的企業身份認證環境是由各種記錄系統組成，其中可能包括網路設備、伺服器和雲端應用程式。管理駐留在這些不同系統中的身份是一個巨大的挑戰，這將對用戶、管理員和開發人員產生有巨大的壓力。此外，當今許多最具破壞性的安全漏洞都是由於用戶帳戶和密碼被盜用而導致，而這些漏洞又因用戶被授予不適當的存取層級而加劇。安全和有效地管理所有系統和應用程式的身份授權，對減少漏洞防護至關重要。

Fortinet 身份和訪問管理 (IAM) 解決方案用於：

- 透過登錄、多重身份驗證 (MFA) 和授權建立身份
- 從身份驗證來源提供根據角色的資訊，以便在特權存取中使用
- 建立並實施根據角色的最低存取策略
- 透過對單點登錄 (SSO) 的支援提供更高的安全性，幫助提高用戶合規性和採用率

3. Network Access Control 網路存取控制

NAC 網路存取控制是一種零信任網路存取解決方案，幫助企業跟上當今不斷擴大的攻擊面。它提供了對網路環境的可視性，以便實施和動態策略控制。無論設備是從網路內部還是外部連接，FortiNAC 都可以自動響應受損設備或異常活動。使用 FortiNAC，企業可以：

- 識別、分析和掃描所有設備的漏洞
- 建立並確保持續不斷的網路控制
- 建立並實施策略，將網路存取限制為僅訪問該設備所需的內容
- 維護自動響應和協調網路

4. Application Access Control 應用程式存取控制

在零信任模型中，應用程式存取應該在每個連線基礎上進行控制，並且應該驗證每個用戶與設備是遠端連接還是從內部網路連接。應用程式存取應反應到每個人的角色，以便只有那些與用戶相關的應用程式可用。應用程式可以駐留在本地伺服器、私有雲或公共雲中，並且仍然由 ZTA 機制進行控制。借助 Fortinet ZTA 解決方案，應用程式存取控制可用於各種部署場景，包括 SASE 服務或本地設備或虛擬機 (VM) 防火牆。

這些解決方案包括：

- 為每個應用連線驗證用戶與設備
- 根據策略控制用戶對應用程序的存取
- 無論用戶身在何處，都能執行應用程式存取策略在用戶與 ZTNA 代理點之間建立安全、自動的連接
- 與防火牆、虛擬機防火牆和 SASE 服務協同工作

對於許多組織而言，這些攻擊凸顯出需要更好的方法，來保護其網路免受保護薄弱的家庭網路連線造成的威脅。[4]

Fortinet ZTA 架構的主要優勢

為了實現有效的安全性，企業必須從保護安全範圍轉向保護分佈在數十億個邊緣、用戶、系統、設備和關鍵應用程式上的資料。Fortinet 平臺跨設備、用戶、端點、雲端、SaaS 和基礎架構，提供全面的可視性和保護。

Fortinet ZTA 框架具有以下主要優勢：

- 對存取應用程式的用戶進行全面、持續的控制，無論這些應用程式駐留在何處或用戶在何處
- 對網路上的用戶進行完全和持續的控制
- 對網路上的內容進行完整和持續的控制
- 針對 Fortinet 安全織網整合的 ZTA 解決方案，可在 LAN、WAN 和遠端隧道上同等工作
- 單一供應商的完整、整合的解決方案

總結

憑藉數十年幫助企業維護網路安全的經驗，Fortinet 提供高效的 ZTA 框架，在四個關鍵領域提供可見性和控制：應用程式存取、網路上的用戶、網路上的設備以及這些用戶與設備的離線活動。

[1] "2019 Zero Trust Adoption Report," Cybersecurity Insiders, November 2019.

[2] Larry Ponemon. "The state of endpoint security risk: it's skyrocketing," Ponemon Sullivan Privacy Report, May 2020.

[3] "2020 Data Breach Investigations Report," Verizon, May 2020.

[4] "Global Threat Landscape Report," FortiGuard Labs, August 2020.

FORTINET

www.fortinet.com/tw

August 17, 2021 2:59 PM

885304-B-0-EN