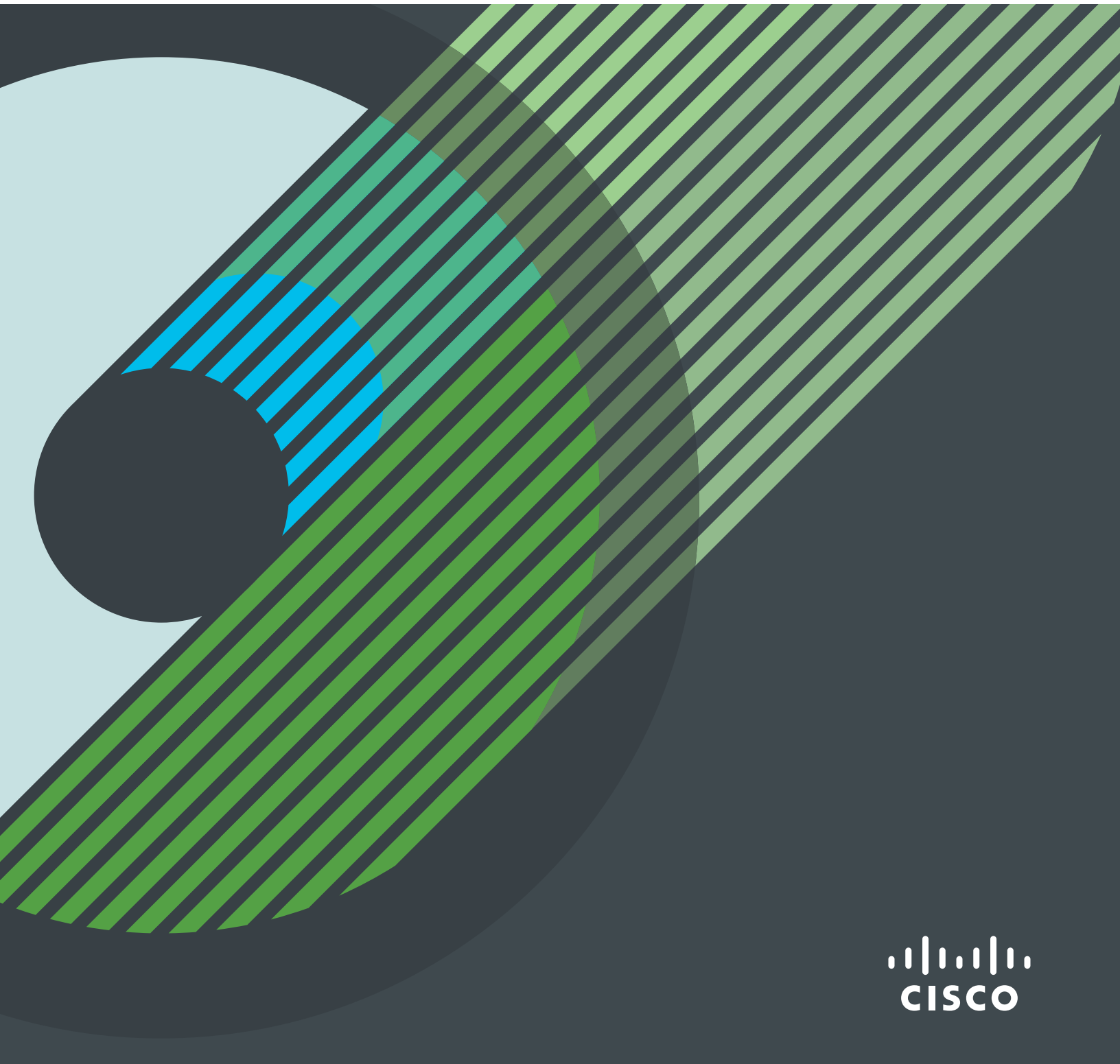
零信任

突破傳統安全的框架



零信任

讓安全突破傳統的邊界

AUTHORS

J. Wolfgang Goerlich
Wendy Nather
Thu Pham

0.0

為什麼選擇零信任？

我們通過一條無形的分界線來劃分屬於企業以及不屬於企業的東西（伺服器、桌上型電腦、網路、應用程式和登錄名稱），這條分界線的安全通常由防火牆以及部署在終端的安全軟體來保護，但是當我們看到屢屢登上新聞頭條的那些案例就能發現，這些防護措施還遠遠不夠。多年來，人們一直在為推進這一邊界的消失而努力:比如為了解決“去邊界化”問題，早在2003年就開始舉辦的論壇 - Jericho Forum)。隨著雲作為一種資料存儲和處理平臺而被人們日益接受，這種思維才真正得到企業的關注。弗雷斯特研究公司（Forrester Research）的首席分析師約翰·金德維格（John Kindervag）在2009年左右就率先提出了“零信任”這一術語，並基於該術語設計了一個特殊的安全框架。谷歌公司不僅針對這一原則的內部落實做了詳細描述，還賦予它一個特有的名稱 - BeyondCorp。當下，這一原則的可行性已經擴展到越來越多的企業組織，企業在考慮如何落實這套方案時，也掌握了可供參考的具體應用實例。

企業在面對消除邊界這一理念時，通常比較猶豫，尤其是在他們最近才對這一邊界加以鞏固的情況下。

所以，我們不要認為這個原則是在消除邊界，而是要借助這一原則來強化企業的內部安全，這樣一來，網路邊界就再也不是阻擋惡意攻擊的唯一屏障了。

傳統方法

用於保護企業資訊資源的傳統方法一般會做以下幾點假設:

1.訪問企業資訊資源的終端設備，其所有權、授予權和管理權均歸企業所有。

2.所有使用者、設備和應用系統的位置均是固定且可預測的，通常由企業網路防火牆提供防護。

3.初始訪問只需一種驗證方法。

4.同一類別的企業管理系統從本質上可以相互信任。

這些年來我們逐漸意識到，由於移動技術、BYOD、雲計算的不斷發展以及合作夥伴間協作關係的日益密切，這些假設已經不再適用。在 IT 日趨消費化的大背景下，用戶不僅追求個性化更強的網路環境，又希望在使用個人設備時免受企業的管制。惡意攻擊者在成功突破一個驗證點（例如防火牆或用戶登錄名）之後便能利用網路固有的信任漏洞，通過在網路、應用或環境中橫向移動來鎖定敏感性資料目標。在受信任區域內發起攻擊的內部威脅則可以獲得更高的權限。我們再也不應認為“內部”實體都是可信任的，不能以為只要對這些實體實施直接管理就能降低安全風險，或者只需要一道驗證就足以抵擋威脅。

走向零信任安全

金德維格將“從來不信任,始終在驗證”規定為“零信任”的指導原則。換句話說，假設您網路中的每個部分都存在潛在威脅（就像直接訪問Internet一樣），您就必須對訪問請求進行相應地處理。針對那些想方設法繞過防火牆（例如，通過遭洩漏的用戶憑證或易被攻擊的 Web 的應用程式）或在企業內部“受信任”網路中發起的威脅，我們應當通過可防止威脅橫向移動的額外安全控制措施對其加以阻止，從而將安全性漏洞所產生的影響降到最低。

網路邊界，與其將它視為圍繞網路“邊緣”的一種存取控制類型，倒不如把它用作制定存取控制決策的平臺。這道邊界仍然可以是防火牆或交換機，但也可能是其他層：在登錄協力廠商 SaaS 應用程式時，使用個人 ID 與使用公司 ID 之間的區別不僅決定了哪些安全決策適用，還決定了這些決策由誰來制定。應用程式試著訪問資料庫的地方，是邊界。用戶為執行敏感操作而提高許可權時，也是邊界。每次出現訪問事件時，零信任安全模型都會提醒您質疑原有的信任假設。

零信任安全方法

搭建零信任模型，要遵循以下幾項基本原則：

- **以洞察指導策略。**為技術管理人員提供盡可能豐富的情報和洞察，以便在制定策略時有理有據。
- **信任不是二進位的，亦不是恒久不變的。**這就需要我們不斷地對使用者、設備和應用程序的狀態進行反復評估，並對信任度做出相應的調整。通過遏制新發現的威脅和漏洞，隨時做好準備，以應對那些使網路風險級別升高的安全事件。
- **所有權不等於控制權。**從 BYOD和 IoT（物聯網）設備到 SaaS 和公有雲，驗證並將信任擴展到所有權或管理權並不掌握在企業手中的設備、應用和網路。
- **邊界為您做出存取控制決策提供了廣闊空間。**選擇最適合企業網路環境的層和流程點，包括網路層、應用層、身份驗證點、以及交易處理工作流程。
- **訪問決策的制定以每一次重新建立起的信任為基礎。**組內成員資格、層內應用服務、或連接到某個網路位置的設備，本身都不足以對活動進行授權。
- **有效遏制。**將最低許可權和分段與各種響應能力結合起來，以及時監控威脅活動，並積極限制威脅活動的蔓延。

除了要質疑所有信任假設之外，您在執行該模型時最好還應具備以下特徵：

- **透明化。**安全措施應盡可能在無形中為技術使用者提供保障[1]。
- **以零接觸支撐零信任。**通過合理化、自動化、編排、集成來盡可能降低管理壓力。

實施成果

採用零信任模型後，您在處理每一次訪問請求時都要對使用者、設備、容器、網路和應用程序的安全狀態進行驗證，從而說明您獲得更全面更深入的洞察。

您可通過細分資源以及僅批准必要許可權和流量的方式來縮小企業的受攻擊面。如果您同時採用更多身份驗證因素、加密措施並對已知和受信任設備進行標記，就能有效增大惡意攻擊者收集所需資料（使用者憑據、網路存取權限和橫向移動能力）的難度。

最後，無論用戶身處何處，正在使用哪種終端設備，將應用程序部署在本地還是雲，他們都可以獲得完全一致且效果更好的安全體驗。

[1] 有些專家也將其稱為“半透明化”：應當具備足夠的可見性，以便用戶在必要時能夠因知道安全措施的存在而感到安心。

零信任安全三大支柱：簡介

安全不應當是一刀切的主張，即使在相同的企業環境下亦是如此。舉個例子，連續身份驗證機制能夠一直保持非常理想的效果：但是如果多種因素身份驗證過於頻繁，用戶勢必感到厭煩（而且會試著規避相關控制手段）。

再看軟體，頻繁的身份驗證對軟體來說並不構成問題，因此彼此通信的工作負載足以為這類交互提供支援。物聯網設備（例如醫療設備或製造設備）可能會因安全性和可用性問題而影響它們的連網方式。在此，我們希望借助零信任安全的三大支柱來簡單說清楚其中的差異：

01

面向企業員工的零信任安全

指那些使用個人設備或企業管理設備訪問工作應用程序的員工、承包商、合作夥伴和供應商。這項支柱能夠確保只有授權使用者和安全設備才能訪問應用程序，而無需考慮位置因素。

02

面向工作負載的零信任安全

指那些在雲、資料中心中以及可實現彼此交互的其他虛擬環境中運行的應用程序。這項支柱重點在於確保 API、微服務或容器在訪問應用程序中的資料庫時的訪問安全。

03

面向辦公場所的零信任安全

這項支柱重點在於確保連接企業網路的任何設備（包括 IoT）的訪問安全，例如使用者終端、實體和虛擬伺器、印表機、攝影機、空調系統、終端機、輸液泵、工業控制系統……

在以下章節中，我們將按照目標風險、實施方案和建議成熟度對每個支柱進行細分。

	目標人群或物件	信任驗證時刻	目標地點
企業員工	人員及其設備	訪問應用程式	任何地點
工作負載	應用程式、服務、微服務	與其他系統通信	本地、混合雲、公有雲
辦公場所	IT 終端及伺服器、物聯網（IoT）設備、工業控制系統（ICS）	訪問網路	本地、混合雲、公有雲

1.0
面向
企業員工

目標風險

面向企業員工的零信任
安全方案可為企業化解以下幾大風險:

+ 重要的帳戶憑證（即用戶名和密碼）在很多時候都是通過網路釣魚攻擊或被攻擊的協力廠商遭到竊取，然後被遠端惡意攻擊者(包括僵屍網路)重新使用。威瑞森（Verizon）2019年資料洩露調查報告指出，近三分之一的資料洩密事件都存在帳戶憑證被盜的情況，這就表明密碼是一種可突破傳統邊界防禦機制、並在不被發現的情況下順利訪問應用程序的一種有效手段。

+ 如果惡意攻擊者能夠突破防火牆，或在企業內網中發起攻擊，那麼這種攻擊會逐漸擴散並破壞關鍵系統，從而竊取敏感性資料。**而我們需要做的則是以實際而言：局外人只要偽裝地足夠完美，便很難將其與局內人區分開來。**外部攻擊者可通過相同的方法混進合法用戶的工作中，因此您必須對每個用戶的操作許可權加以限制。

+ 惡意攻擊者還會利用適用於同類資產的不同策略或執行方式之間的差異，這是另外一重風險。如果在採用不同類型身份驗證的兩個不同的系統中允許使用相同的機密資料，那麼惡意攻擊者肯定會選擇更容易竊取的資料-要麼是由於它信任可被您利用的其他資訊，要麼是由於某種身份驗證方法存在固有缺陷。如果某個應用程序或系統處於不同控制項的保護下（具體取決於用戶是否位於“邊界內”），那麼惡意攻擊者則會把比較薄弱的一組控制項作為攻擊目標。

+ 基於雲的外部應用和移動用戶則要面臨企業邊界保護機制之外的重重攻擊。

+ 如果使用者使用非託管及未修復設備存取關鍵系統和資料，極有可能會將企業置於危險的境地。這些薄弱點會導致勒索軟體攻擊、其他類型的惡意軟體攻擊、以及未經授權的訪問。

概述

要落實面向企業員工的零信任安全方案，離不開合法終端設備以及使用它們的合法用戶。而這些設備和它們所訪問資源之間的端到端加密手段，則會讓原有的防護如虎添翼。

最後，僅允許按用戶的角色所需為其分配最低存取權限（也稱為“最小許可權”）。只要按照正確數量的身份因素進行用戶驗證，並且使用已註冊且經過安全性漏洞檢查的終端設備，惡意攻擊者就能通過一個集中的代理精確存取他們已被授權訪問的那些資源。

員工零信任安全成熟度模型

第1階段　構建用戶信任

務必採用正確的機制和流程，以確保只有授權使用者才有許可權訪問企業資源。雖然實現這一目標的途徑有很多種，但比較常見的還是多因素身份驗證（MFA）技術。

第2階段　設備及活動可見性

每一次存取請求都來自哪個端點或哪台設備？它當前的安全狀態如何？請求具體來自什麼位置？這個過程就是檢測帳戶接管威脅和其他風險的關鍵階段。

第3階段　可信任設備

無論是否歸企業所有，無論託管還是未託管，企業組織都可以將自己已註冊並希望與特定使用者相關聯的設備標記為受信任設備。

第4階段　適應性策略

根據資源的敏感性和已知的安全狀態實現訪問要求，以便根據風險等級作出適當的管理。從僅授權企業管理設備到要求特定版本的補丁軟體、加密手段或基於用戶行為的遞升式認證，策略的範圍甚是廣泛。

第5階段　面向企業員工的零信任安全

至此，所有應用程序和系統在前面列出的階段中都已提及；對風險事件的監測和回應也一刻沒有停止；且所有用戶都能擁有一致的單點登錄體驗。

2.0
面向

工作負載

目標風險

面向工作負載的零信任
安全方案可為企業化解以下幾大風險:

- 如果惡意攻擊者利用了應用程式的漏洞，就能通過橫向移動來攻擊各種關鍵系統。
- 惡意攻擊者竊取並外泄敏感性資料。
- 內部應用和外部雲應用間迥然不同的控制項成為網路安防人員的盲點。
- 開發人員要對 Web 應用程序進行編碼和配置，從而讓企業面臨被攻擊的可能。
- 54%的 Web 應用程序漏洞容易被惡意攻擊者利用，這意味著如果伺服器和應用程式未經過修復，就會暴露在已知漏洞中，惡意攻擊者正是利用這些漏洞入侵您的系統。

概述

企業的系統往往是有機的：它們在功能上不斷豐富，並根據具體的業務需求增加連接和依賴項。為了促進企業系統這種良性的增長，系統設計人員和開發人員有時會傾向于採用最寬鬆、最靈活的安全配置。由此產生的過度信任會被惡意攻擊者利用，然後再通過橫向移動順利訪問企業的敏感資源。

解決這個問題的最佳答案即網路分段。比如由展示層、應用層和資料層組成的通用三層 Web 應用程式。

我們可將這幾層劃分為不同的網路，並通過特定的訪問控制項來限制層與層之間的通信方式。這個示例即便比較簡單，應用層上的服務由於要與同一層上的其他服務進行通信，因此會被信任，這樣一來便不利於解決在層內橫向移動的風險。應用程序越來越複雜，數量越來越多，過度信任問題也會隨之增加。而且，久而久之，企業很可能會搞不清哪些才是關鍵性工作負載，其他哪些資源需要與之通信，因此要準確鎖定它們，更是難上加難。

這些問題理論上有兩種解決方法。我們可以假設網路是不受信任的，並將信任決策向上移至應用堆疊。這種方法的優點在於我們可以將控制措施植入應用程式。而缺點就是必須在實施零信任安全方案後才能進行應用程式的開發。開發人員不會一直記錄應用程式應當如何與其自身的工作負載進行通信，更別說如何與外部資源通信了；鑒於這一點，網路和安全運營團隊如果想知道如何在最小許可權和應用可用性之間掌握好平衡就更加困難。

另外一種方法就是通過僅根據應用程式的需要來限制通信，以此降低網路內部的信任。這種方法非常適合現有的應用程式（包括舊版本），並且有助於將現有生態系統引至零信任模型之中。這種方法的缺點就在於我們需要依靠網路安全機制，而且即使這道安全防線被突破，應用程式服務也不會發現安全機制被削弱這一危險的情況。

這兩種方法並非相互排斥，在需要通過冗餘控制項來滿足高安全等級要求的環境中，二者可能會更好地彼此平衡。

為了將現有環境向零信任模型引導，我們的網路必須要在網路通信點完成信任評估和存取控制決策。考慮到我們的應用服務通常分佈在雲服務商、資料中心和其他虛擬化環境中，因此要做到這一點這絕非易事。我們需要定義一個應用程式生態系統，使其僅容納應用程式的依賴項，包括服務、流程和網路通信。然後，我們就能通過白名單或預設拒絕模式來進行存取控制，而且能夠在不考慮網路或環境的情況下，都只對應用程式所需的資源進行授權。**在明確信任等級時，我們的依據並非網路的位置，而是應用程式的具體要求。**

微分段技術的實現需要三種技術，而且就算當下，這些技術仍遙不可及。

- **深入、廣泛的網路通信洞察。**以分散式網路感測器代替傳統的中央監控系統（SPAN / TAP 或 NetFlow），從而使大規模深入洞察成為可能。
- **精確、即時的應用程式建立。**大資料分析技術大大減少了人工記錄應用程式的工作量，從而說明使用者及時瞭解流量模式及依賴關係。
- **跨多個環境中的多台設備應用策略的能力。**高級策略引擎可防止存取控制設備在多個多雲環境中無序蔓延，由此簡化了應用程式的洞察和分析步驟。

洞察、分析、策略，三者結合，由此降低了應用程序生態系統中存在的過度信任。

但是，如果出現信任濫用的情況，會造成怎樣的結果？ 舉個例子，假設企業面臨管理人員和其他特權用戶帶來的風險，而這部分使用者往往在較大範圍內都享有較高的存取權限。任何會威脅到開發人員或管理員身份憑據的外來入侵者都可能獲得存取權限，而安全操作人員對此可能毫不知情。即使為安全操作團隊配備負責檢查單個工作負載和連接情況的專人，也無法徹底解決這個問題。為了面向工作負載實現零信任安全，思科通過無人監管的機器學習技術和行為分析技術來監控惡意活動的跡象。一旦發現惡意行為，網路就會立即隔離相關服務並阻止通信，以此來撤銷信任。

變化的速度一旦超出了人們的能力範圍，人們必然會選擇通過自動化技術來解決問題。而這就網路分段技術當下的發展狀態。如果從零信任的角度進行思考，系統設計和開發人員也能找到解決問題的新思路。面向工作負載的零信任安全憑藉更優質的洞察、更快速的分析以及對應用通信更深入的瞭解，圍繞預期行為重新定義了什麼是邊界。從最初的威脅到橫向移動再到資料洩露，惡意活動在整個過程中都清晰可見，因此可防可控。

工作負載零信任安全成熟度模型

第1階段　構建工作負載信任

查明具有關鍵任務工作負載的應用程式生態系統和環境。這個階段主要明確零信任方案的範圍。

第2階段　工作負載可見性

深入洞察應用環境中的設備、流程、資料封包、網路流以及工作負載的通信情況。這項工作僅限於應用程式生態系統，此外可見性對於深入洞察工作負載（例如未下載補丁程式的軟體以及配置狀態）也至關重要。

第3階段　對應應用程式依賴項目

在分析網路通信和資料流程的基礎上完成應用建立，對應用層進行分類，並找出應用程式依賴項目。這些工作需要一段時間才能完成，目的就是要捕獲那些不常見的活動，例如月度工作或季度會計流程。應用程式序對應的結果越準確，得到的策略就越正確。

第4階段　策略及微分段

在對源自企業員工及辦公場所相關支柱的身份及上下文資訊加以適當考慮的前提下，制定相應地策略以盡可能降低應用程式生態系統中的信任，執行策略模擬及驗證，並面向所有環境完成一致的策略部署。微分段技術以流量白名單（也稱為默認拒絕）為核心，旨在根據工作負載的具體需求對訪問邊界進行相應的移動。

第5階段　面向工作負載的零信任安全

在零信任安全方面已經比較成熟的企業會對企業的各種環境進行持續改進和即時監控。俗話說，唯一不變的就是改變 – 應用程式、企業組織、惡意攻擊都會發生改變 – 因此，隨著生態系統的日益演變，零信任安全需要策略也隨之演變。

3.0

面向

辦公場所

目標風險

面向辦公場所的零信任
安全方案可為企業化解以下幾大風險:

- 惡意攻擊者利用終端、伺服器或設施設備的漏洞在網路中站穩腳步，並通過橫向移動來破壞關鍵系統。
- 惡意攻擊者攻擊通過網路而相互連接的業務基礎設施，從而干擾正常操作。
- 物聯網或運營技術（OT）存在薄弱環節。
- 據調研公司 Quocirca 稱，有百分之六十的企業都經歷過因網路印表機產生的安全事件。
- 據卡巴斯基（Kaspersky）稱，2017至2018年間，新的 IoT 惡意軟體變種數量已增長了三倍。

概述

現代辦公場所通常以校園、資料中心、WAN、分支網路和雲網路為使用場所。信任被擴展到任何使用者、設備和應用程式，再通過有線或無線方式連接其他使用者、設備、應用程式以及辦公場所的其他部分。辦公場所中會佈置一些最終使用者設備、IT服務器和印表機、工業控制系統（ICS）以及 IoT 設備。無論哪一類設備在企業網路上進行身份驗證和通信，面向辦公場所的零信任安全方案都將及時強制實施信任。

但是，員工使用的設備和安裝在辦公場所中的設備，二者之間的確存在明顯的差異。我們可以對面向終端使用者應用的訪問決策強制實施信任，但這種思路並不適用於印表機、生產控制設備、環控設備、標記閱讀系統等設備。為了覆蓋所有與業務相關聯的系統，我們需要將堆疊的底層移至網路。

我們在設備管理、設備修復以及非法設備防禦方面的能力已經不足以應對網路中數量激增的設備。而近年來網路設備的爆炸式增長，也讓物聯網得到了廣泛關注。物聯網通常建立在消費級平臺上，缺乏企業級安全控制措施，並且可能無法修復。而這就會帶來一種結果：我們擁有了更多類似的設備，這些設備平均每台的漏洞數量相對更高，而且要維護 Internet 的安全也相對更加困難。在物聯網成為人們關注焦點的同時，我們也不能忽視印表機、視訊會議、安防攝影系統、VoIP 電話等一系列傳統的商業設備，因為這些設備仍然為犯罪分子入侵企業網路提供了可行途徑。此外，我們需要考慮的還有醫療設備和 OT。出於操作、功能和技術方面的許多因素，這些設備通常部署在安全團隊無法修復或保護的平臺上。從廣義上講，面向辦公場所的零信任安全性原則必須能夠跨越所有設備實現身份驗證、授權、分段和信任監控。

零信任假定網路本身是不安全的。當使用者、設備和應用程序連接網路時，我們需要對網路進行保護，反之亦然。在零信任網路中，任何有漏洞的設備均要被遮罩或分段，以降低它們被犯罪分子發現和利用的可能性。此外，在零信任網路中，還要防止其它設備免受被攻擊和遭利用設備的影響。這兩套保護措施密切相關，而且都需要我們掌握使用網路的所有已知實體以及設備的安全狀態。

當設備試著連接網路時，就需要做出存取控制決策。網路工程師們往往會通過某些固定屬性（例如，網路交換機所在位置或 IP 位址的組合）來完成此任務。在這個模型中，我們在對設備進行信任時，並不瞭解它們是否存在漏洞或已遭惡意利用。傳統的信任模式所依據的屬性也通常很有欺騙性。企業在向零信任過渡的過程中，信任決策必須根據許多因素來做出，比如身份和行為，而且需要根據設備行為和任何不斷變化的因素進行定期驗證，尤其是要通過限制原始網路存取權限或完全切斷其訪問路徑來應對新查明的威脅和漏洞。

網路存取控制（NAC）構成了實現零信任安全的基礎。在這個模型下，設備必須先對網路進行身份驗證，才能被信任，然後連接網路並進行通信。通過802.1X和基於憑證的身份驗證搭建起的軟體定義存取控制框架就是一種理想的方案。而 Windows 設備則能利用活動目錄和 Windows 管理規範（WMI）對網路進行身份驗證。如果這些方法不可用，我們也可以選擇 MAC 旁路認證（MAB）。雖然 MAB 具有一定的欺騙性； 但是，對於不支援新方法的老舊設備，或我們無法通過配置讓設備支援這些新方法，那麼它可能就是唯一的選擇。

零信任網路的下一個層次便是基於組的分段網路。我們會對各種網路連接進行驗證。在做出訪問決策時，網路會根據設備隸屬的一種或多種角色，以及它們隸屬的一個或多個組別，對設備的身份進行標識。設備所隸屬的角色與 IP 位址或實際位置無關。在大部分結構比較複雜的企業中，這些角色通常包括多個子網和多棟建築。然後，我們就能根據哪些實體組能與哪些網路資源（包括互聯網）進行通信來定義網路分段策略。我們可以根據設備的行為判斷設備的受信任程度，並在出現風險因素時再進一步限制對設備的訪問。此外，我們還能通過持續的通信監控以及持續的策略集改進，不斷降低網路中的假設信任，同時強化網路內部的安全。

伴隨員工自有設備的劇增，企業網路中的設備數量也相應地增多。從物聯網到印表機，從 OT 到醫療設備，支撐企業正常運營的設備比以往任何時候都要更多。正因為如此，由設備所創造的攻擊面也比以往任何時候更大。面向辦公場所的零信任策略能說明安全操作人員和網路工程師更好地瞭解所有主機設備和通信資料，對網路通信實施更嚴格的限制，並根據信任度執行相應的自我調整策略。 然後，我們就能夠有效降低這些設備遭惡意活動利用的風險，並針對任何可疑流量做出更及時的回應。

辦公場所零信任安全成熟度模型

第1階段　構建辦公場所信任

搞清楚部署在辦公場所中的系統、這些系統的使用者及相關應用程序，包括 IoT 和 OT，並確定其在企業組織中的功能及其在網路上的操作。明確零信任安全方案的適用範圍。

第2階段　網路可見性

深入洞察辦公場所網路環境中使用者、設備和應用程序的通信以及網路流量。瞭解並記錄適用範圍內的網路功能及要求。

第2階段　網路存取控制

面向適用範圍內的使用者（如果有）、設備及應用程序配置並實施網路身份認證和授權。防止任何未經身份認證（並因此不受信任）的實體連接適用範圍內的網路。

第3階段　分段策略

定義基於群組的網路策略，確保這些策略僅允許業務運營所必需的網路連接和通信。

第5階段　面向辦公場所的零信任安全

企業向零信任安全過渡的最後一個階段即持續改進。及時根據設備、功能及企業需求的變化，不斷調整適用的範圍、設備和策略。

4.0

總結

採用零信任安全解決方案，您的基礎設施無需經過整體改造。因為最成功的解決方案應當在混合環境的頂層為其提供支撐，而不是完全取代現有的投資。

儘管要與整個環境的不同部分協同，必然需要使用不同類型的策略創建和執行方法， 因此跨各種執行點共用與使用者、設備和應用程式相關聯的身份、漏洞和威脅的動態上下文才是協調安全性原則的最佳途徑。

思科零信任

思科零信任提供了一種綜合全面的安全方法，旨在確保面向企業應用程式和網路環境的所有訪問存取，無論來自哪一位使用者、哪一台設備、哪一個位置，都安全可靠，從而為企業員工、工作負載和辦公場所提供全方位保護。

- **Duo 為企業員工提供保護。**通過基於 Duo 的零信任員工安全性原則，思科就能確保只有合法的使用者和安全的設備才能訪問應用程式，而無需考慮它們的具體位置。
- **Tetration 為工作負載提供保護。**通過基於 Tetration 的零信任工作負載安全性原則，思科就能確保企業應用程式內部以及在整個多雲環境和資料中心內，所有連接都是安全可信的。
- **軟體定義接入 (SD-Access) 為辦公場所提供保護。**通過基於 SD-Access 的零信任辦公場所安全性原則，思科就能確保整個網路上所有的使用者和設備（包括物聯網）連接都是安全可信的。

這套完整的零信任安全模型能說明使用者減輕、偵測並應對整個環境中的不同風險。

瞭解有關**思科零信任**的更多資訊。