ActualTech Media

Hewlett Packard Enterprise 慧與

即使花費重金，中小企業也難以實現滴水不漏的安全性

Ed Tittel

目錄

內容摘要

慧與可以協助中小企業 (SMB) 建立並維護營運安全性，從容面對勒索軟體、網路釣魚、資料洩漏、駭客攻擊等持續增加且日益猖獗的威脅。

中小企業必須尋求專家協助，才能解決因為人員短缺和技能差距而無法迅速應對安全性事件，從而付出高昂代價的困境。本文將探討慧與如何協助中小企業解決這些難題。

重要內容包括：

- 從靜態的被動式安全性轉變為隨需應變的智慧型安全性
- 利用涵蓋邊緣、雲端和內部部署環境的全方位安全性措施，彌補 IT 安全性差距
- 定義涵蓋安全性、合規性、IT 永續性和災難復原的安全性策略
- 將安全性深植在 SMB 結構中

數位世界四處危機重重。所有企業和組織都遭遇來勢洶洶、令人畏懼的安全威脅現況，中小企業 (SMB) 也不例外。一如最近所有安全性調查所發現的結果，各種規模的組織無不面臨數量、種類和兇猛程度都不斷增加的威脅，惡徒甚至不斷擴大攻擊面。

> **在 IT 員工難以跟上需求的環境中，大多數的中小企業發現自己只能被動地對安全性警示做出反應，而無法以主動和先發制人的方式管理威脅並解決潛在的漏洞。**

根據 Forrester 發佈的《2020 年安全營運狀況報告》指出，在過去 12 個月，有 79% 的企業曾經發生某種類型的安全入侵事件，而資料洩露仍是所有企業最念茲在茲的問題。此外，安全性團隊及企業主也面臨巨大的技術難題，這些難題大多起因於工具太過複雜或各行其是，不僅導致效率低落，更造成安全性漏洞百出。該研究也發現，最新的五大安全性威脅如下 (按類型列出)：

1. 勒索軟體：這類惡意軟體會對業務資料和系統進行加密，必須支付解密費用才能復原，但就算付了錢也不保證一定能成功救回資料
2. 網路釣魚：透過電子郵件、網頁或社群媒體廣發連結，誘使警覺性不高的使用者點進惡意網站，然後竊取密碼和認證資料(甚至是更機密的資料)
3. 資料洩漏：讓業務資料悄無聲息穿越組織防線，進而落入不肖分子之手的非法手段
4. 駭客攻擊：鎖定 IT 基礎架構的技術和社群工程進行攻擊，旨在獲取控制權；拒絕存取或拒絕服務；以及竊取資料、智慧財產或金錢
5. 內部威脅：來自前員工或現任員工的攻擊，這些員工通常心懷不滿，並利用內部技能及知識來設法得到業務資料、IP 或財務資產

大多數組織 (據 Forrester 報告，有 83% 的組織) 其實都設置了某種類型的全年無休安全防護機制，但往往因為缺乏適當的技術和人員，而無法因應數量和嚴重程度不斷增加的網路攻擊。事實上，許多企業都苦於應付每天必須處理的安全性警示數量。

中小企業也有為數不少的安全性問題

中小企業特別容易受到各種安全性問題的困擾，因為 IT 人員編制較少，人員不是欠缺安全性專業，就是嚴重過度負荷。在 IT 員工難以跟上需求的環境中，大多數的中小企業發現自己只能被動地對安全性警示做出反應，而無法以主動和先發制人的方式管理威脅並解決潛在的漏洞，

中小企業因此極有可能蒙受災難性損害或損失。根據 Ponemon Institute 的報告顯示，2020 年每起資料洩露的平均成本為 386 萬美元。對於營運規模較小的企業來說，如此巨大的損失直接悠關公司的存亡與否。此外，某些攻擊 (如勒索軟體) 可能讓中小企業陷於癱瘓，使其根本無法營業。將這種攻擊稱為大災難，絕非誇大其辭。中小企業也需要安全保護，以避開潛在的法律和法規風險，否則涉及客戶資料的資料洩漏不僅也會招致這些風險，同時還要承擔巨額的財務罰款，以及對企業聲譽的損害。

實際上，對安全性攻擊或資料外洩的回應速度不夠快，就可能給中小企業帶來一場浩劫。損失業務產生的機會成本，再加上維修、復原和報告 (以及潛在的後續追蹤稽核) 成本，以及其他成本等，這些都對利潤影響甚鉅。這說來話長，簡單說就是想要確保萬無一失的安全性可能所費不貲，而且會佔用大量資源，但不採用安全性措施或採用將就的安全性措施，付出的代價可能更高，甚至可能威脅到企業能否存續。

中小企業的邊界不斷向外延展

從前，中小企業只要全神貫注於自己的組織邊界就能高枕無憂。確保邊界安全可以解決大多數安全性問題並化解很多風險。如今，無所不在的資料和應用程式，讓一切變得難以追蹤和保護。在疫情當道下，員工幾乎都是遠端工作，這意味著每個裝置的每一次使用，都需要保護。由於網際網路是將使用者與應用程式和服務緊密連結的重要媒介，因此安全通訊比以往任何時候都更加重要。此外，不論是在內部部署環境中還是在一或多個雲端 (目前大多是多個雲端) 上，確保其中的儲存裝置和伺服器安全無虞，也同樣至關重要。簡而言之，當組織的資產、應用程式和員工隨時隨地運作時，安全性和保護就是讓一切保持正常運作的關鍵所在。

HPE 安全性解決方案

慧與隨時可以協助中小企業實現重要轉變，將靜態且孤立的被動式安全性工具和技術，轉換為縱橫數位世界的隨需應變智慧型安全性平台。慧與的安全性解決方案可讓中小企業透過覆蓋邊緣、雲端和內部部署環境的安全措施，在一致且連貫的安全性保護傘下，彌補現有的安全漏洞。為達成這個目標，慧與提供以下功能：

- 以資料為中心的安全性：使用經過實證的 NIST 標準化方法來保護使用中的資料、靜態資料和移動中的資料 (符合美國政府和歐盟 GDPR 要求)。這提供了強大的加密和權杖化功能，讓攻擊者無法使用竊取而來的資料。
- 零信任安全性：這是一種用於身分識別和存取權管理的理性方法，系統預設不信任所有使用者或軟體動作。因此，任何使用者、裝置和應用程式執行個體都必須證明自己的身分和授權，才能獲准存取。
- DevSecOps：在正式的開發流程中引入安全性概念並全程由安全性團隊監督，如此可確保及早解決經常在整個應用程式交付鏈 (從設計、建置、測試、交付到維護) 中出現的安全問題，而不是在開發結束時，才將安全性團隊和概念直接強加到系統或服務「成品」上。慧與制定了一套 DevSecOps 最佳做法 (**圖 1**)，可在開發和部署過程中解決安全性問題。

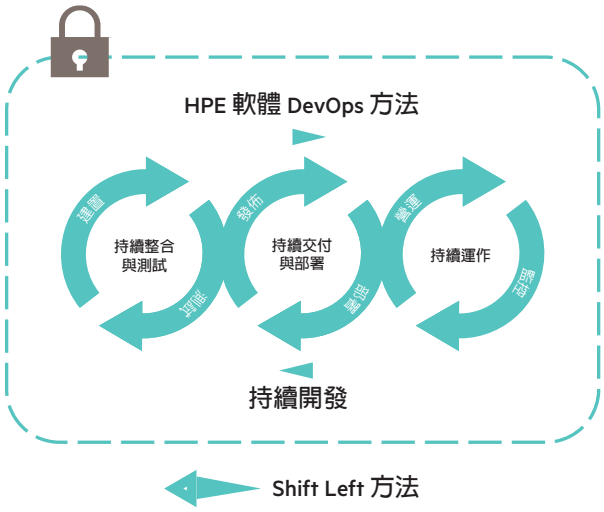

圖 1：DevSecOps 是 DevOps 基本概念的延伸，目的是建立「資訊安全，人人有責」的觀念

慧與值得信賴的供應鏈計畫

為了滿足客戶需求，協助其解決高安全性要求和具有挑戰性的使用情況，慧與隆重推出值得信賴的供應鏈。這類客戶包括美國聯邦和公共部門的使用者，他們更喜歡美國出產且保證可驗證網路的產品。將安全性深植於供應鏈的方法是，納入其他強化的安全性功能，並指派慧與員工在製造流程期間監督產品，以仔細檢查所有零件、觀察組裝，並確保封裝後的裝置在客戶接受交貨之前保持原狀並且無任何損害。慧與擁有獨家的矽晶片信任根 (Silicon Root of Trust) 技術，這項技術可將基於矽晶片的安全性嵌入到產業標準伺服器中，並在整個供應鏈中保持安全性控制，以建立並維護嚴格的硬體層級安全性。

慧與甚至使用正式記錄、經常稽核的安全性供應鏈，來解決自身產品開發和交付中的安全性問題 (請參閱：「**HPE Trusted Supply Chain 計畫**」)。

> **慧與隨時可以協助中小企業實現重要轉變，將靜態且孤立的被動式安全性工具和技術，轉換為縱橫數位世界的隨需應變智慧型安全性平台。**

慧與也提供 PointNext 諮詢服務，協助中小企業稽核、定義及精簡安全性策略。我們的專家可隨時協助您確保安全性原則滿足整個組織的安全性需求，以及符合隱私權、保密和資料保護的合規要求。這些專家還可以協助中小企業以經濟實惠的方式，將卓有成效的業務永續性和災難復原選購產品，整合到可能實作的任何隨需應變的智慧型安全性平台中。他們可以為中小企業提供安全性藍圖，讓中小企業用作自己設計和實作的基礎，並協助中小企業透過測試、試行和生產部署來實現。

在邊緣打造第一道安全防線

總而言之，慧與會和中小企業攜手合作，將安全性深植到整個組織的每個角落。也就是說，遠端員工將可以安全可靠地作業，所倚靠的就是深植並蘊含在邊緣、內部部署和混合式雲端環境中的安全性。這種方法會將安全性深植到整個 IT 基礎架構中，不論是架構實體還是顯露出來的氣勢，都讓人同感安全可靠。因此，HPE Edge 深植於內的安全性，能夠確保邊緣運算功能一經啓動，即可隨著部署和演進而持續保持安全，這些邊緣運算功能包括智慧型工作場所、IoT 環境、虛擬桌面基礎架構，以及 Microsoft (Teams、Exchange、Microsoft 365)、VMware、Linux 虛擬機器等的服務交付。HPE 資料中心，以及包括 HPE GreenLake、HPE InfoSight 在內的許許多多雲端/混合式雲端解決方案，也是如此。

> **慧與會和中小企業攜手合作，將安全性深植到整個組織的每個角落。**

請造訪慧與的安全性與數位保護服務頁面，查看各種安全性藍圖、HPE 安全性產品組合、案例研究等資訊。