INFORMATION TECHNOLOGY INTELLIGENCE CONSULTING（資訊技術智慧諮詢股份公司）

ITIC 2021 全球伺服器硬體、伺服器作業系統安全性報告

2021 年 6 月

目錄

目錄 2
執行摘要 3
引言 6
威脅全覽：安全漏洞和資料外洩是最重大、最昂貴的可靠性威脅 8
伺服器供應商：IBM、聯想、華為和 HPE 強化安全性 10
資料與分析：供應商安全性成效 11
平均偵測時間是關鍵指標量表 13
結論 22
建議 25
方法 27
調查人口統計資料 27
附錄 28

執行摘要

連續第三年，企業將 IBM、聯想、華為和 HPE 的關鍵任務伺服器評為最安全的平台（按此順序），成功的資料外洩次數最少，駭客也最難破解。

在最新 ITIC 全球伺服器硬體安全調查中，比較了 15 種不同伺服器平台的安全性和功能， ITIC 的獨立網路調查自 2021 年 1 月起至 2021 年 6 月中旬，對全球 28 個不同垂直市場領域的 1,100 多家企業進行了訪談與調查。

儘管過去 18 個月內，在 COVID-19 疫情全球大流行的期間，資安駭客和資料外洩事件顯著增加了 42%，但 IBM、聯想、華為、HPE 和 Cisco，仍是鶴立雞群、保持最可靠和最安全伺服器平台的領先地位。

以 IBM Z 為首的頂級伺服器，以及 IBM POWER、聯想 ThinkSystem 和華為 KunLun（按此順序），均在 ITIC 的最新調查中，取得 COVID-19 疫情中各自的最佳安全性和可靠性/執行時間效能，並在所有 15 個主流伺服器硬體平台中的每個安全指標，都取得了最佳安全性結果，包括：

- 最少次數的資安駭客成功入侵/資料外洩事件。
- 最少的非計畫性伺服器停機時間。包含***任何***原因造成的整體非計畫性停機，以及因安全事件而導致的非計畫性停機。
- 最快的平均偵測時間 (MTTD)。偵測時間係指 從攻擊開始，至公司將其隔離並關閉間的時長。

- 最快的平均修復時間 (MTTR)。修復時間係指讓伺服器、應用程式和網路恢復到完全正常運作的時長。
- 最少量的安全資料外洩，包括因勒索軟體、網路釣魚詐騙或 CEO 詐騙等，造成的丟失、被盜、毀壞、損壞或變更。
- 最少量的金錢損失，因資安駭客入侵成功所致。
- 最高信心水準的伺服器硬體嵌入式安全性，以提供警示/警告、並抵禦安全攻擊和資料外洩。

除了以 IBM Z 為首的頂級伺服器品牌，HPE 和 Cisco 的關鍵業務系統也提供了高階安全性，並在安全伺服器排名中，躋身第五。 另一方面，白牌伺服器（無品牌）再次被證明最容易被滲透，遭安全滲透成功的總數也最高。

ITIC 最近的全球安全調查中發現， IBM、聯想、華為和 HPE 的關鍵任務伺服器，受資安駭客和資料外洩成功入侵，而經歷的停機時間百分比最低（**參見圖 1**）。

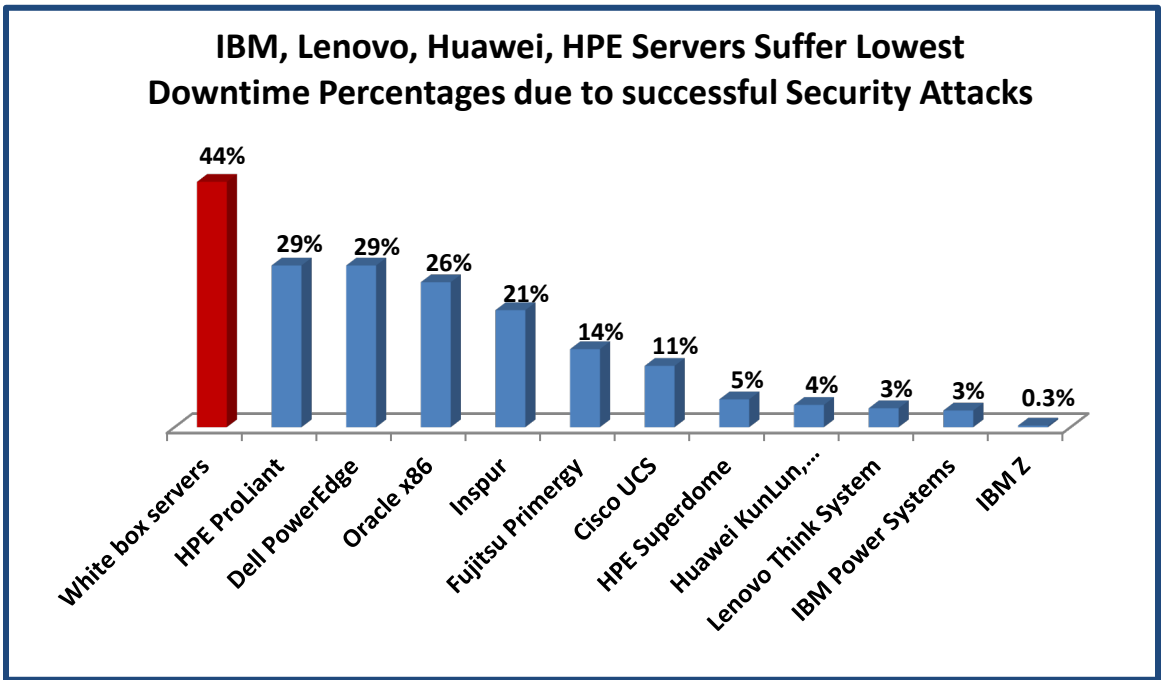
在最新的 ITIC 研究中，IBM Z 大型主機超越了所有其他伺服器發行版，並獲得了迄今為止最強大的安全性和可靠性評級，在同類產品中獨樹一幟，其他品牌望塵莫及。

擁有卓越安全性——只有 0.3% 的 IBM Z 高階伺服器，成功遭受資料外洩。 在其他主流硬體平台中，只有 3% 的 IBM Power Systems 和聯想 ThinkSystem 用戶的系統被成功入侵，而近 4% 華為崑崙和 5% HPE Integrity Superdome 伺服器用戶受到一次成功的侵害。

超過 10% 或 11% 的 Cisco UCS 伺服器被成功入侵， 儘管 Cisco 的硬體表現出色，考慮到許多 UCS 伺服器部署在偏遠地區和網路邊緣，但這通常也是第一道防線，首當其衝地

受到駭客攻擊。白牌伺服器最容易受到安全滲透，高達 44% 的受訪者表示有被成功入侵的經驗。

圖 1. IBM、聯想的伺服器最為安全、最難破解



來源：ITIC 2021 全球伺服器硬體、伺服器作業系統安全性報告

總體而言，ITIC 的調查結果表示，在效能最佳的平台和最不安全的產品之間，伺服器硬體安全性和可靠性之間存在顯著且持續擴大的差異。 全球疫情大流行引發了一波與 COVID-19 相關的資料外洩、勒索軟體、網路釣魚、商業電子郵件入侵 (BEC) 與 CEO 詐騙和攻擊，出現頻率有增無減。

ITIC 最近的調查結果表示，可靠性和安全性密不可分、一體兩面。 安全威脅和資料外洩會立即破壞受威脅的伺服器、應用程式和網路，影響運行時間和可用性， 安全駭客和資

料外洩的代價高昂且危險， 他們損害了企業的智慧財產權 (IP) ，甚至是業務合作夥伴、客戶和供應商的智慧財產， 而資安駭客入侵成功也可能揭露員工的個人資料。

前五名最可靠的伺服器平台：IBM Z、IBM Power Systems、Lenovo ThinkSystem、Huawei KunLun 和 Fusion Servers、HPE Superdome Integrity 和 Cisco UCS（按此順序）同時擁有最強大的安全性，這當然不是巧合。

引言

全球疫情大流行引發了一波與 COVID-19 相關的資料外洩、勒索軟體、網路釣魚、商業電子郵件入侵 (BEC)、CEO 詐騙和攻擊，這些攻擊針對無數的跨產業企業和消費者裝置和軟體，且有增無減、持續蔓延。

沒有人能夠倖免， 這使得固有的、健全基礎架構之安全性，勢在必行。

ITIC 的最新調查發現，總體而言，73% 的受訪者擔心他們的組織將在未來 12 至 18 個月內，成為專業駭客針對性攻擊的受害者， 這個時間表與從幼兒園至高中三年級學校、大學、已經完成遠距學習的師生，現正準備返回課堂的普遍趨勢吻合， 同樣地，許多企業和政府機構正轉移到混合居家遠距辦公，作為一種健康安全的措施。

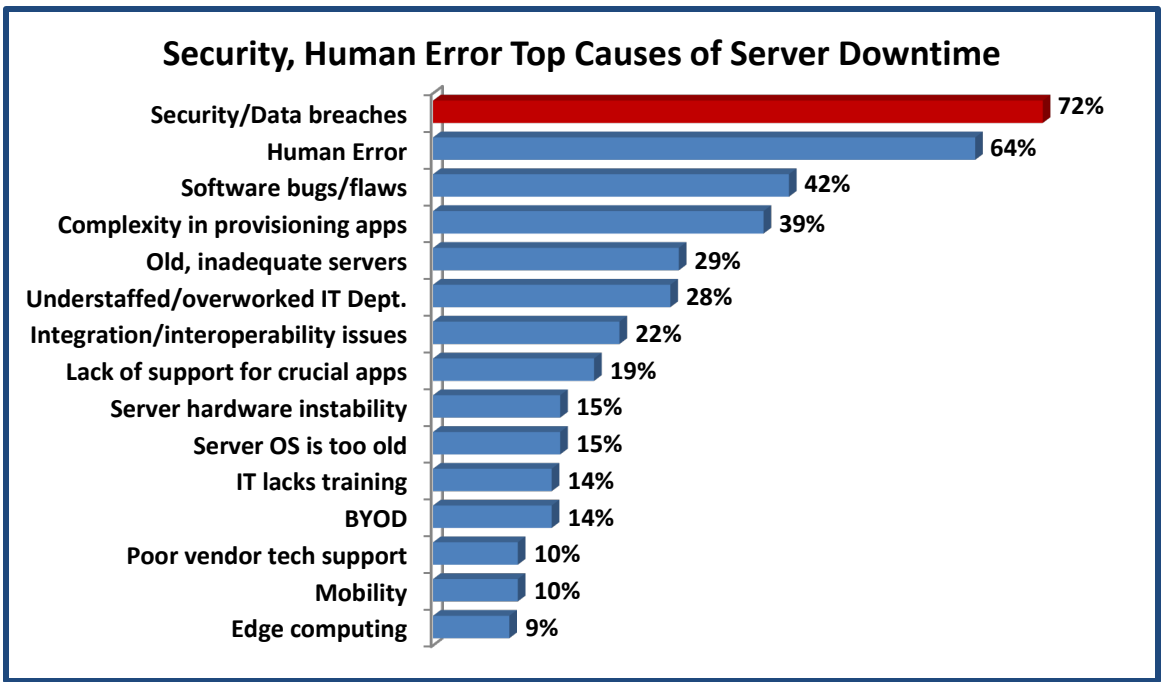
ITIC 最新的安全調查結果，得到了自 2020 年初已發佈多個網路安全風險警示的數個美國聯邦政府機構的大力支持： 聯邦調查局（FBI）、 國土安全部網路安全和基礎設施安全局 (CISA) 、證券交易委員會 (SEC) 合規檢核辦公室 (OCIE)。

根據 FBI 於 5 月和 6 月發布的警報，與 COVID-19 相關的網路安全威脅包括針對失業保險和聯邦經濟刺激檢核、保健醫療、銀行、銀髮族、加密貨幣和政府詐騙計畫等。 FBI 點出了「.....犯罪分子在疫情期間，針對居家受教育的兒童，進行線上掠奪性行為」的實例。

IBM、聯想、華為、HPE 和 Cisco（按此順序）發布的強大安全結果尤其值得注意，因為它們發生在 COVID-19 疫情大流行的高峰期間。 大約 40% 的受訪者表示，自 2020 年初 COVID-19 疫情開始以來，他們的伺服器、作業系統和關鍵業務應用程式，更常被資安駭客成功入侵。 在 ITIC 2020 年全球伺服器硬體、伺服器 OS 可靠性調查中，已有 19% 的組織表示他們的伺服器被駭客成功入侵，但 2021 年光是上半年，就已有 31% 表示受害，增加幅度從 9 % 至多到 21 %。

安全性影響了一切的企業技術和業務問題。 約 72% 的受訪者認為安全和資料外洩是對伺服器、應用程式、資料中心、網路邊緣和雲端生態系統可靠性的最大威脅（**參見圖 2**）。駭客入侵更具針對性、普遍性和危害性， 以對其企業和消費者受害者造成最大的損害和損失。

圖 2. 安全性、人為錯誤、軟體錯誤是出現運作中斷時間的主要原因



來源：ITIC 2021 全球伺服器硬體、伺服器作業系統安全性報告

威脅全覽：安全漏洞和資料外洩是最重大、最昂貴的可靠性威脅

對於新興的專業駭客社群，資料外洩是一筆大生意和主要業務。 駭客入侵在許多方面要付出非常昂貴的慘痛代價， 根據 IBM 和 Ponemon Institute 聯合進行的 2020 年資料外洩成本研究， 2020 年資料外洩成本為 386 萬美元[1]， 自 2015 年以來增加了 10%。 實際成本因駭客入侵的持續時間和嚴重程度，而有所不同。 勒索軟體攻擊不斷激增，

[1] 「2020 年資料外洩的成本研究」， IBM 和 Ponemon Institute。 URL: https://www.ibm.com/security/data-breach

且代價不菲。 DarkSide 駭客在 2021 年 5 月 7 日發起的勒索軟體攻擊，使 Colonial Pipeline Co. 關閉了六天[2]， Colonial Pipeline 供應了美國東海岸從新澤西州到佛羅里達州 45% 的天然氣和柴油燃料， 它關閉傳送並導致包括佛州、北卡和弗吉尼亞州等州內，出現天然氣的嚴重短缺， 最終只有當 Colonial Pipeline 執行長 Joseph Blount 同意支付 440 萬美元贖金時，噩夢才落幕。 布朗特告訴《華爾街日報》，他授權支付 440 萬美元的贖金，是因為高階主管們不確定網路攻擊對系統的破壞程度， 以及需要多長時間才能恢復管道。

Colonial Pipeline 勒索軟體攻擊只是眾多攻擊之一， 可見到安全攻擊成功相關的漏洞、風險和高成本， Colonial Pipeline 勒索軟體駭入，進一步強化刺激人們對一流、強大的安全基礎架構的需求—— 而伺服器硬體正是每個企業網路和生態系統的基礎架構元素。

一份 DTEX 系統報告發現「只有 30% 的組織準備好確保完全轉移到遠端工作。」 DTEX Systems 的研究還發現，近 75% 的組織擔心在家遠距工作者，會帶來的安全風險，73% 的企業承認，若他們的 VPN 被遠端工作人員停用，他們將無法看見使用者的活動。 另一個令人震驚的發現是，遠距工作人員將工作電腦用於個人用途，25% 的受訪者承認這會增加風險，15% 的受訪者表示他們的公司因此更容易受到網路釣魚的攻擊。

ITIC 的最新研究表示，停機時間的單位小時成本持續攀升， 對 89% 的中小企業和大型企業都超過了 300,000 美元。 總體而言，42% 的大中型企業受訪者表示，平均小時的停

[2] 「Colonial Pipeline CEO 講述了他為何向駭客支付了 440 萬美元的贖金」，華爾街日報，2021 年 5 月 19 日。 URL: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

機時間，會使公司損失超過 100 萬美元， 在最壞的情況下，高峰使用時間若發生中斷關鍵業務營運的資料外洩，很可能使企業每分鐘就損失達數百萬美元。 任何因有針對性的勒索軟體攻擊，而遭受數小時或數天長期中斷的組織，幾乎肯定會遭受百萬美元等級的損失。

除了因生產力和營運中斷所致的明顯經濟損失外，企業還必須考慮其他機會成本，如參與補救工作和恢復營運的 IT 和安全管理人員的工時與人數， 公司還必須確定任何資料或智慧財產權 (IP) 是否丟失、被盜、損壞、毀壞或變更， 也必須增加任何訴訟成本、安全事件和資料外洩相關的潛在民事或刑事罰款， 又如對組織聲譽的損害，這是無法計算的，更可能會導致長久且不可逆的業務損失。

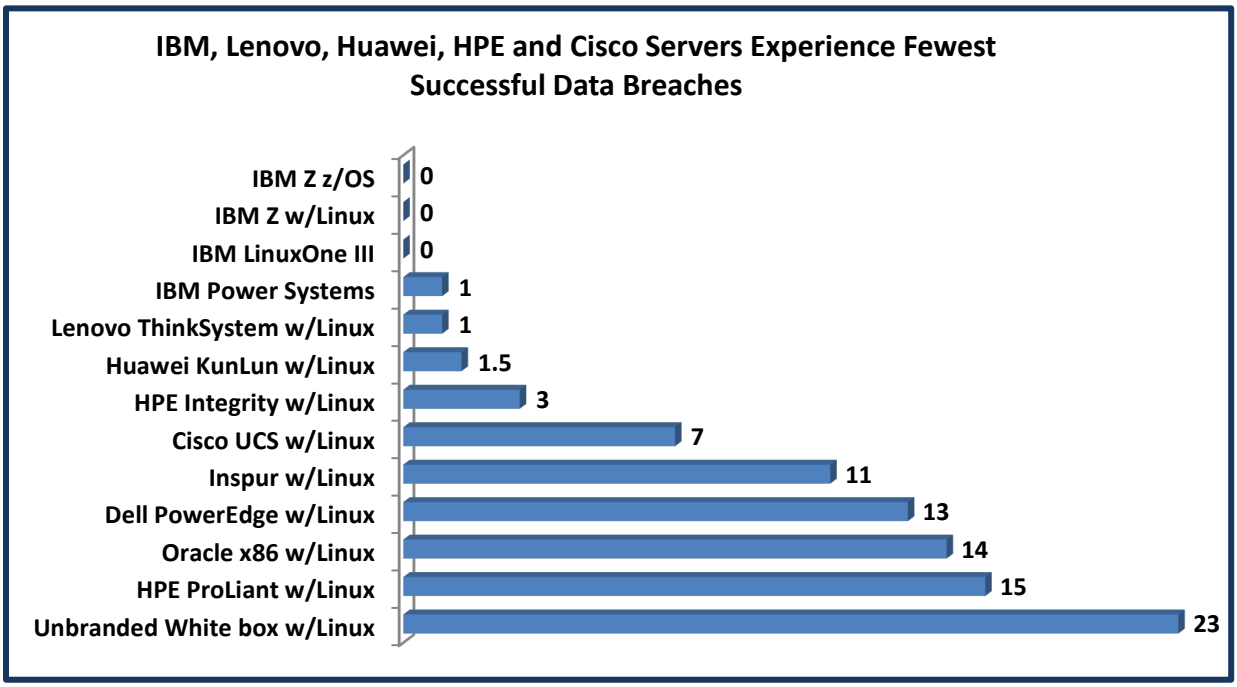
駭客極度精確地挑選目標，並迅速利用每個機會， COVID-19 疫情情境就是一個典型的例子： 駭客立即將目光盯上了遠端工作和參加在線課程的遠距學習， 他們瞄準了這些所謂的「軟目標」—— 地方政府、中小型學區、醫院與醫療保健診所、醫生辦公室和銀行分行辦公室，大多缺乏全職現場安全和 IT 管理者，並且沒有最新的安全性防護。

伺服器供應商：IBM、聯想、華為和 HPE 強化安全性

IBM、聯想、華為、HPE 等長期獲得最高伺服器可靠性評級的供應商，也是最安全的硬體平台，這點並不令人意外。 這些頂級供應商，加上最近的 Cisco 、聯想 Case 伺服器、PC 和筆記型電腦，將安全性列為重中之首，並在過去幾年內，投入巨資加強產品供應項目固有的安全性。 因此，當 COVD-19 疫情來襲時，它們已經擁有強大的嵌入式安全性，讓它們處於有利的領先地位。

如**圖 3** 所示，最安全的伺服器硬體平台成功遭到安全侵害的情況最少， 執行 z/OS 和 Red Hat Enterprise Linux (RHEL) 的 IBM Z 以及 IBM LinuxONE III 的受訪者都表示，這些平台在過去 16 個月沒有被資安駭客成功入侵， 緊隨其後的是 IBM Power Systems 和 Linux ThinkSystem 伺服器，各有一台；華為 KunLun 平均兩次駭客攻擊；HPE Integrity 有 3 次遭到滲透，Cisco 的 UCS 伺服器則有 7 次資料外洩。 白牌伺服器的漏洞最多，在過去 16 個月中平均發生 20 次成功的資料外洩。

圖 3。 IBM、聯想、華為伺服器受成功駭客入侵的次數最少



來源：ITIC **2021** 全球伺服器硬體、伺服器作業系統**安全性報告**

資料與分析：供應商安全性成效

誠如前段所言，ITIC 2021 年全球伺服器硬體安全性調查發現，IBM Z、IBM Power Systems、聯想 ThinkSystem 和華為 KunLun 和 Fusion 伺服器（按此順序）在每個安全種類中，都取得了最佳結果，包括：

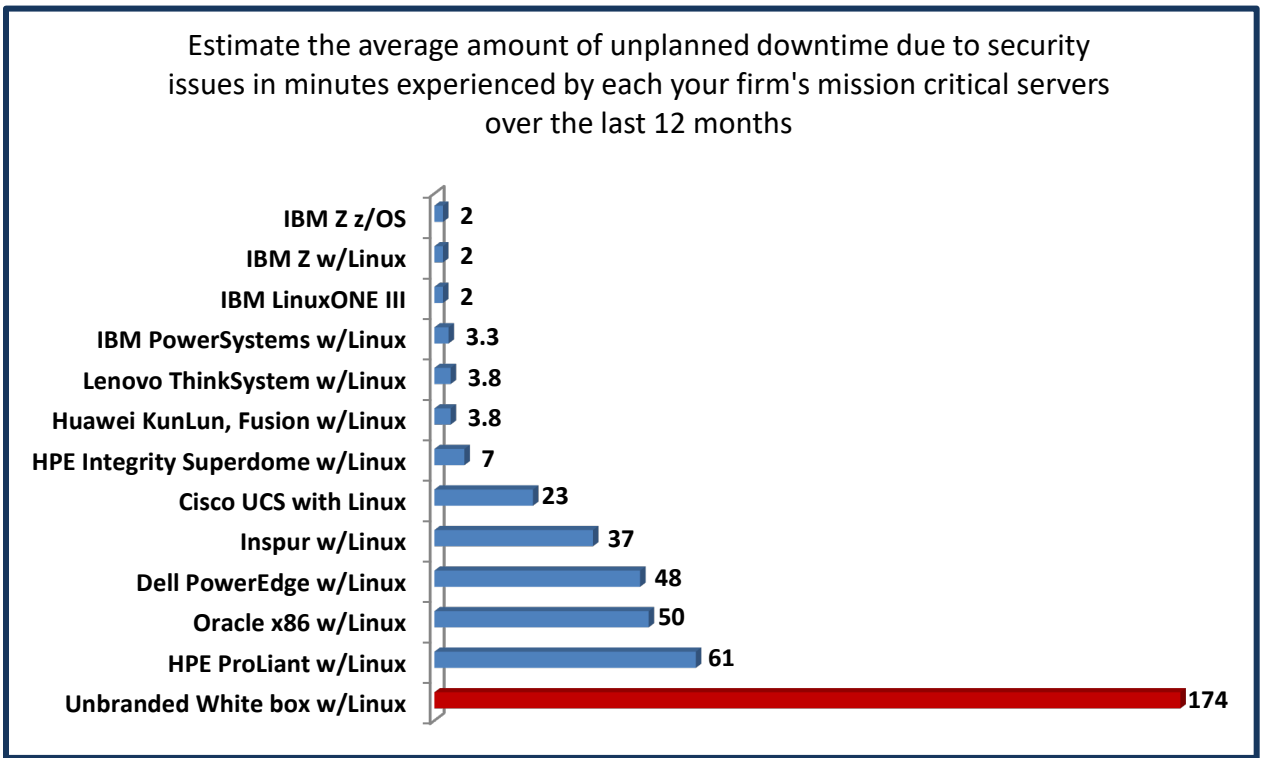
- 最少次數的資安駭客**成功**入侵/資料外洩事件
- 最少的非計畫性伺服器停機時間。包含***任何***原因造成的整體非計畫性停機，以及因安全事件而導致的非計畫性停機。
- 最快的平均偵測時間 (MTTD)。偵測時間係指 從攻擊開始，至公司將其隔離並關閉間的時長。
- 最快的平均修復時間 (MTTR)。修復時間係指讓伺服器、應用程式和網路恢復到完全正常運作的時長。
- 最少量的安全資料外洩，包括因勒索軟體、網路釣魚詐騙或 CEO 詐騙等，造成的丟失、被盜、毀壞、損壞或變更。
- 最少量的金錢損失，因資安駭客入侵成功所致。
- 最高信心水準的伺服器硬體嵌入式安全性，以提供警示/警告、並抵禦安全攻擊和資料外洩。

如**圖 4** 所示，IBM Z、IBM Power Systems、聯想 ThinkSystem 和華為 KunLun 關鍵任務伺服器，安全事件和資料外洩導致的非計劃性停機時間最短。

IBM Z 和 IBM LinuxONE III 總體上每台伺服器，平均只有 2 分鐘的非計劃性停機時間；緊隨其後的是 IBM 的 POWER8 和 POWER9 伺服器，每台伺服器經歷了 3.3 分鐘的意外服務中斷；Lenovo ThinkSystem 硬體和華為 KunLun 和 Fusion 伺服器經歷了每台伺服器平均 近 4 分鐘的非計劃性停機時間。 白牌伺服器在許多執行上未經許可的伺服器作業系

統和軟體應用程式版本，由於安全問題而導致的運作中斷時間長達 174 分鐘或近 3 小時。 這使得最安全的 IBM Z 伺服器的安全性和可靠性，比起最不安全的白牌硬體高了 87 倍，而 IBM POWER8 和 POWER9 產品的安全性，也比無品牌白盒伺服器高了 58 倍。

圖 4. BM、聯想和華為提供頂尖一流的伺服器安全



來源：ITIC 2021 全球伺服器硬體、伺服器作業系統安全性報告

平均偵測時間是關鍵指標量表

安全駭客和資料外洩，是數位時代實際開展業務必會發生的情況。 在某些時候，每個組織及關鍵主要事業單位的伺服器、伺服器作業系統和應用程式，都將成為某種形式上資料外洩企圖或入侵的受害者。

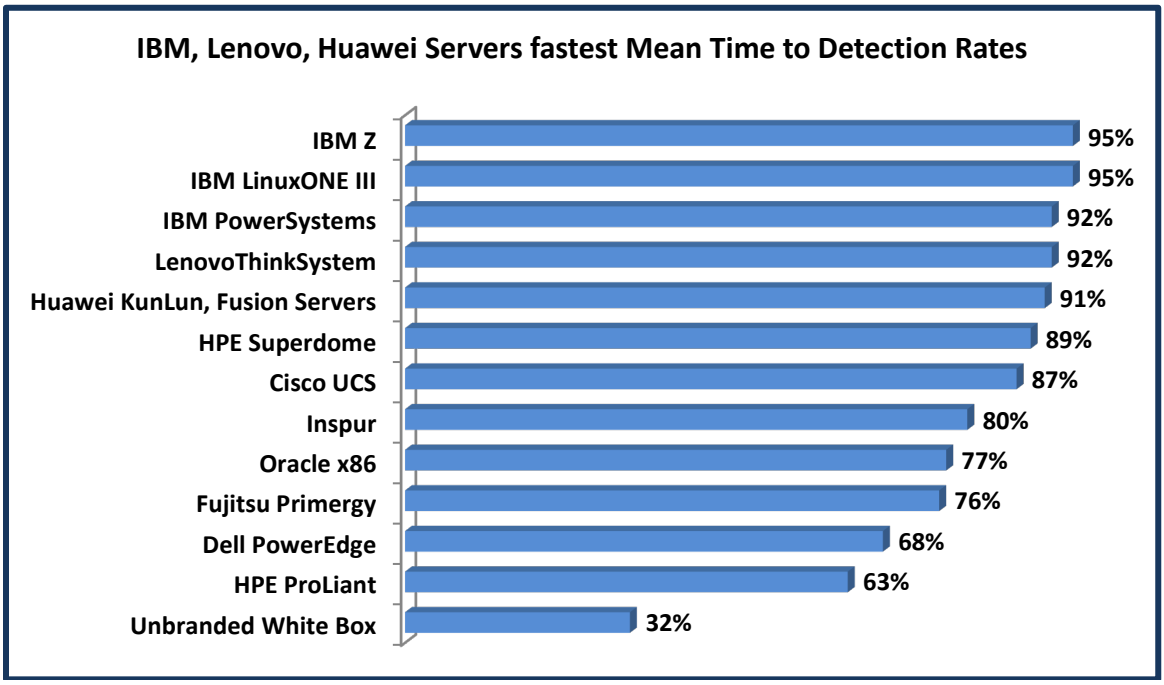
組織必須仰賴強大的內嵌伺服器和基礎架構安全性，來識別危險，傳送警示和警報，並具有隔離威脅的能力。 充分準備以及擁有訓練有素的安全專業人員和 IT 管理者員工，對企業與組織而言至關重要。

企業伺服器和軟體，能偵測到安全問題並做出回應的速度越快，在攻擊滲透到網路生態系統、中斷資料交易和日常營運、存取敏感資料和 IP ***之前***，隔離和阻撓攻擊的機會就越大。

圖 5 顯示，IBM Z、IBM Power Systems、Lenovo ThinkSystem、Huawei KunLun 和 Fusion Servers（按此順序）在阻止駭客攻擊方面表現出色。 在所有伺服器平台中，這些伺服器的平均偵測時間 (MTTD) 百分比最高。

95% 的 IBM Z、IBM LinuxOne III 調查受訪者表示，他們的伺服器能夠「立即或在前 10 分鐘內」偵測到駭客的安全侵害企圖並將其關閉。 IBM Power Systems、Lenovo ThinkSystem 和華為 KunLun 發行版平台使用者中，有 92% 表示他們能夠「立即或在前 10 分鐘內」識別並抵禦安全侵害。 關鍵核心基礎架構伺服器、作業系統和關鍵任務應用程式抵禦駭客攻擊的速度越快，企業幾乎不會發生停機時間，也幾乎不會成為被盜、更改、損壞、資料遭盜用和智慧財產遭竊的受害者。

圖 5. 超過 90% 的 IBM、聯想和華為伺服器「立即或在前 10 分鐘內」偵測到安全攻擊



來源：ITIC 2021 全球伺服器硬體、伺服器作業系統安全性報告

伺服器供應商的安全性成效評量

IBM 安全性 關鍵成效

- **IBM Z** 伺服器在所有伺服器平台中，整體可靠性、可存取性、效能和安全性方面，持續達到一流水準。 IBM Z 系列 – "Z" 代表零停機時間 – 在每個可靠性類別中，始終優於**所有**競爭對手，並提供最低的總擁有成本 (TCO) 和最快的投資報酬率 (ROI)。 z13、z14 和 z15 Systems 伺服器的可靠性/執行時間、應用程式可用性評級和安全性，在每台伺服器/每年停機時間的實際非計劃性中斷分鐘數方面，得分最高。 IBM z 大型主機和 IBM LinuxONE 發行版，均表現出真正的容錯率，僅經

歷 0.6 分鐘——每台伺服器每年因伺服器缺失而導致的***非計劃性***停機時間不到一分鐘，而 Z 和 LinuxONE 平台平均為 0.74 秒（ITIC 2019 年全球伺服器可靠性調查）。 雖然每台伺服器停機時間，與去年同期相比減少 0.14 秒，聽起來微不足道，但實際上它減少了近 19%，並將 IBM Z 和 LinuxONE 的 TCO 降低了 230 美元 – 從 2019 年的每台伺服器每分鐘 1,232 美元降至每台伺服器 1,002 美元（最新的 ITIC 2021 全球伺服器硬體安全調查）。 IBM Z 所記錄的每月停機時間僅為 4.32 秒，幾乎無法察覺。 鑑於安全駭客和資料外洩的持續激增，IBM Z 伺服器配備最高的安全性，此點相當重要， 從 2021 年 1 月至 6 月中旬，Z 持續保持資料外洩的最低百分比、不到 1%， 此外，IBM Z 和 LinuxONE III 受訪者還提到了最快的平均偵測時間 (MTTD)，其中 95% 的 ITIC 企業受訪者表示，他們的安全和 IT 管理者能夠偵測並提早阻止駭客入侵。 一言以蔽之，這些成效突顯了 Z 和 LinuxONE III 產品的成功與卓越。 IBM 2019 年收購 Red Hat 也為平台提供了支援，讓 Z 和 LinuxONE 平台上的 Linux 工作負載顯著增加， IBM 高階主管公開表示 Linux MIPS 增長了 55%。 在 IBM 前 100 名 Z 客戶中，有 92 家執行 Linux 工作負載， 並且，根據 IBM 所稱，Z 平台平均每年有 100 到 200 個全新部署。

- **IBM's LinuxONE III** 是基於 IBM Z 的開放式平台， 專門針對混合雲環境並利用 Z 的全面加密。 LinuxONE III 平台和 IBM z15 還包含 IBM Hyper Protect Data Controller，可提供透明的端對端、資料級保護和隱私權， IBM Hyper Protect Data Controller 使企業能夠加密資料、授予和撤銷對資料的存取權限，並保持控管 – 即使資料從記錄系統中移出時也一樣。 IBM LinuxONE III 在 ITIC 2021 年的調查中，分享了最高的安全性和可靠性排名，95% 的 LinuxONE III 企業在攻擊發生後「立即或在前 10 分鐘內」偵測並停止了資料外洩。
- **IBM Power Systems** 92%的 IBM Power Systems 客戶表示，他們的 IT 和安全管理者能夠在發安全侵害時，「立即或在前 10 分鐘內」偵測到並阻止攻擊。 IBM 的 POWER9 橫向擴充系統已經推出三年，下一代 Power10 伺服器於 2021 年秋季

發行上市。 IBM 不斷刷新和更新產品線，特別強調效能、對關鍵任務工作負載、進階分析、記憶體內資料庫和嵌入式安全的支援。 所有 Power Systems 模型均為雲端就緒， 且 IBM Power Systems 在堆疊所有層中（處理器、系統、韌體、作業系統和 Hypervisor）都內建了安全性， 透過晶片內建的加速加密技術，您的資料在動態和靜止的情況下，都能受到保護， IBM 也聲稱其 PowerVM Hypervisor 沒有被報告的安全漏洞。 POWER9 伺服器是雲端就緒，包含內建的 PowerVM 虛擬化功能， 而橫向擴充伺服器專門用來整合到組織的雲端和 AI 策略， 這提供了支援任務關鍵工作負載（如 IBM 的 Db2 和 Oracle 資料庫、SAP HANA）所需的高效能和 RAS 功能。 Power10 設計為 7 奈米芯片尺寸，兼具能源效率和效能， IBM 估計，與 POWER9 相比，這將使處理器能源效能、工作負載量和容器密度提高多達 3 倍！ 此外，即將推出的 Power10 伺服器還將包含一系列進階功能，包括：支援多 PB 記憶體叢集，這將擴展雲端容量，以支援記憶體密集型工作負載，Power10 還將具有硬體支援的安全功能，如用於端對端安全的透明記憶體加密。與 IBM POWER9 相比，IBM Power10 處理器旨在實現顯著更快的加密效能，每個核心的 AES 加密引擎數量，是 IBM POWER9 的四倍，適用於當今最嚴苛的標準和預期的未來加密標準，如量子安全加密和全同態加密， 它還為容器安全帶來了全新的增強功能。

Lenovo 安全性 關鍵成效

- **聯想 ThinkSystem** 伺服器在所有基於 Intel x86 的伺服器中，實現了最佳 MTTD 率，92% 的調查受訪者表示，他們的 IT 和安全管理者立即或在滲透的前 10 分鐘內，偵測到並停止企圖發動的駭客入侵和資料外洩。 這非偶然—— 自聯想收購 IBM 基於 x86 的伺服器業務以來的七年，以及收購 IBM 個人電腦和筆記型電腦產品線以來的十年中，聯想一直將安全性放在首位， 因此，聯想伺服器和桌上型電腦不斷增強伺服器及桌上型、筆記型電腦的效能、可靠性和安全性。 聯想的技術

服務和支援也是一流， 聯想的 ThinkSystem 伺服器持續改進可靠性，因硬體問題致使的每台伺服器停機時間為 1.51 分鐘， 與 IBM 一樣，聯想建構並執行了卓越有效的安全性戰術和策略。 2018 年，聯想為其 PC 和筆記型電腦推出了 ThinkShield 端對端安全技術。 在過去三年中，隨著安全攻擊的激增，先進的 ThinkShield 技術使聯想 PC 和伺服器保持良好的市場優勢。 在 COVID-19 疫情大流行期間，隨著許多組織轉向為員工和學生提供遠程作業，IT 和安全管理者一直難以跟上資料外洩的步伐， 聯想 ThinkShield 安全性解決方案提供了關鍵支援，如 ThinkShield 在 ThinkSystem SE350 中，佔有舉足輕重的地位， 該型號是聯想首款專門打造的邊緣伺服器，針對網路邊緣提供最佳頻寬、增強安全性並減少停機時間。 ThinkSystem SE350 是一款體積小巧的伺服器， 它高 1.75 英寸，寬 8.1 英寸，深 14.9 英寸，可以可以安裝在牆上、堆疊在架子上或安裝在機架中。 ThinkSystem SE350 專門設計為高效能伺服器， 它基於 Intel 的 Xeon-D 處理器，配備 256GB RAM 和 16TB 內部固態儲存空間， ThinkSystem SE350 增強了實體安全功能，如鎖定框架、入侵偵測、竄改偵測、加密儲存， 它擁有了零接觸部署軟體。 聯想的總體策略融合了創新與可靠、靈活和安全的資料中心系統， 這是一個精明趨勢，也對聯想的伺服器、網路和最終其企業客戶產生了深遠的影響。 迄今為止，人為錯誤是造成伺服器停機時間的最大原因， 傳統上，一般使用者是總體安全鏈中最薄弱的環節之一，尤其是在 COVID-19 疫情期間，絕大部分的一般使用者採遠距辦公，而學生則採遠距學習， 因此，聯想鎖定桌上型電腦和伺服器，對其嚴防禁閉。 聯想在生產製造設施和全球供應鏈，施行嚴格的安全標準、政策和程序， 品質工程師保留隨時審核公司信賴的供應商的權利，使公司能夠進一步控制和洞察其裝置元件的安全性。 ThinkShield 還提供設計層次安全性， 這將安全的 BIOS 和韌體，以及隱私螢幕和筆記型電腦相機快門併入其裝置中，以幫助最大限度地減少行動式使用者在公共場所時的「視覺駭客入侵」。 ThinkShield 旨在保護使用者的身份和憑證，提供 FIDO 認證的身份驗證器並與 Intel Authenticate 整合（提供多達 7 個身份驗證因素）。 ThinkShield 還具有基於

BIOS 的智慧型 USB 保護功能，這是透過將 USB 埠配置為僅回應鍵盤和指標裝置來運作。 聯想還強調其開放式伺服器、儲存設備、網路和系統管理平台與現有和傳統環境無縫整合。 在 ITIC 採訪中，聯想客戶指出易於部署、易於整合和舊版相容性有助於 ThinkSystem 平台的基本可靠性和穩定性。 聯想使用者還提及了廠商優秀的售後服務和支援， 聯想的系統設計支援任務關鍵型資料庫、企業應用程式、大數據分析以及雲和虛擬化環境， 這兩個系統都將眾多容錯和高可用性功能整合到一個高密度、機架優化的無蓋套件中，最大限度地減少了支援「大規模網路運算作業」和簡化服務所需的空間，因為系統永遠不需要從機架刪除。 2020 年 8 月，聯想推出了多款基於 Advanced Micro Devices AMD EPYC 702 系列處理器的 ThinkSystem 單單插槽伺服器全新機型。 聯想伺服器產品組合的新增產品專為處理客戶不斷發展的資料密集型工作負載而設計，例如視頻安全、軟體定義儲存和網路智慧型情報， 他們還支援虛擬化和網路邊緣環境—安全至上， 為那些重視傳輸量和安全性與輕鬆可擴展性的客戶，提供了一個集功能和效率於一身的解決方案。 聯想聲稱這兩款新的 ThinkSystem 伺服器，「以單插槽的成本提供了雙插槽伺服器的效能」，並有可能將客戶的軟體許可成本降低多達 73%，並將 TCO 降低多達 46%。

Cisco UCS 安全性 關鍵成效

- **Cisco UCS** 持續獲得良好得分，並在 ITIC 2020 年全球伺服器硬體、伺服器作業系統年中更新調查中，首次實現了每台伺服器 2.3 分鐘的停機時間， 從 2021 年 1 月到 6 月中旬，Cisco 伺服器穩定地保持在此數值。 考慮到許多 Cisco UCS 伺服器位於處於安全攻擊前線的網路邊緣，這並不容易， 87% 的 Cisco UCS 調查受訪者表示，他們能夠「立即或在前 10 分鐘內」偵測、隔離和停止安全駭客侵入。 Cisco UCS 調查受訪者提及，伺服器在過去 18 個月內，經歷了 7 次被資安駭客成功入侵， 為應對資料外洩的增加，Cisco 開始發佈 Cisco UCS 強化指南， 可供下

載， 這包含幫助使用者保護 Cisco UCS 平台裝置，以提高網路安全性的詳細資訊， 圍繞對網路裝置功能進行分類的三個平面進行結構化，概述了每個 Cisco UCS 軟體功能並參考了相關文件。 此外，Cisco 還推出了多項管理和效能升級，優化擁有總成本 (TCO) 並加快安裝和部署。 Cisco 聲稱其 UCS 將使纜線減少 86%，並允許在幾分鐘內進行配置，同時將資本支出減少 40% 以上， 並向使用者保證組件之間的 100% 相容性， 負載平衡則不會是個問題。

HPE 安全性 關鍵成效

- **HPE Superdome** 伺服器系列（Integrity 和 Flex）為 92% 的客戶，展示了 99.999% 和 99.9999% 的高可靠性。 89% 的 HPE 調查受訪者表示，他們的公司「立即或在前 10 分鐘內」發現並停止了安全侵害， ITIC 意見調查資料顯示，HPE Superdome 伺服器在過去 18 個月內，每部都遭到 3 次被資安駭客成功入侵。 HPE 硬體平台躋身最安全系統中的第五名。 Superdome 產品組合受益於 HPE 硬體固有的強大穩定性， HPE 已將安全性、功能/效能創新和售後技術服務與支援，作為其首要任務， 在日益不安全、複雜和相互關聯的數位時代，這些至關重要。 HPE 在從中小企業到最大跨國企業中都耕耘已久， HPE Superdome Flex 伺服器具有 RAS 功能和端對端安全性，可保護重要工作負載。 HPE Superdome Flex 伺服器可提供多達 32 個插槽的可擴展性， 這是上一代伺服器可擴展性的 2.3 倍， 它還具有記憶體內設計和單個平台中 768GB - 48 TB 的記憶體容量。 HPE Superdome Flex 伺服器採用模組化設計，可以以 4 插槽的增量從 4 插槽靈活擴展到 32 插槽。 HPE 還表示，Superdome Flex 伺服器為 4 插槽的關鍵任務工作負載，提供了更具成本效益的進入點，與以前的型號相比，它的採購成本降低了 45%， HPE 也強調可靠性，提供了 99.999% 的可用性。 HPE 聲稱 Superdome Flex 伺服器透過預測性錯誤處理錯誤分析引擎減少了人為錯誤。 安全和人為錯誤是兩個密切相關的問題，它們關係到安全性和可靠性， 該引擎預測硬體故障，並

啟動自我修復，而不需要人為介入或操作員協助， 它包含韌體層次錯誤，包括記憶體錯誤，發生在使用 HPE 的「韌體優先」方法在作業系統層發生任何中斷之前。 HPE 還透過 HPE Serviceguard for Linux (SGLX) 高可用性和災難回復叢集解決方案為 Linux 工作負載提供持續性。 這使企業能夠保護其執行 Linux 的伺服器免受跨越任何距離的實體或虛擬環境的大量基礎架構和應用程式錯誤的影響。

華為 安全性 關鍵成效

- 在過去的五年華為，總部設在深圳，中國憑藉其高端 KunLun 關鍵任務伺服器和基於 FusionServer x 86 的通用伺服器，成為全球前五名伺服器硬體供應商之一。 根據 ITIC 2021 年全球伺服器硬體、伺服器作業系統可靠性調查和 ITIC 2021 年全球伺服器硬體安全調查，華為崑崙伺服器和融合伺服器，也躋身最可靠和安全的硬體平台前三名。 91% 的華為受訪者表示，他們的 IT 和安全管理員「立即或在 10 分鐘內」偵測到並停止了企圖破壞的行為。 華為受訪者表示，KunLun 和 Fusion 伺服器在過去 18 個月內分別經歷了 1.5 次駭客攻擊。 自 2015 年以來，華為加強了其伺服器的先進特性、內在安全性和整體效能。 為了與 IBM、Cisco、富士通、HPE、浪潮、聯想等對手競爭，華為的伺服器系列包括通用機架和刀鋒伺服器，以及用於解決高效能運算 (HPC) 的關鍵任務硬體， 華為還為其伺服器注入了先進的功能，以支援新興的運算密集型應用程式，如 AI、大數據分析、深度學習和機器學習。 華為強調安全性，它透過「如何建置主動防禦系統」上記載的最佳作法，來提供安全性。 透過其 HiSec 解決方案，支援更具智慧的威脅偵測、威脅回應、安全營運和維護， 華為表示，HiSec 提升了企業網路和電信基礎架構威脅防範能力，從而提高了安全性維運效率，降低了維運成本。 此外，華為為其數據中心、雲和網路中的各種伺服器解決方案提供了許多新的安全產品。

結論

安全性是對伺服器硬體、伺服器作業系統、關鍵業務應用程式的可靠性和可用性，產生負面影響的最大潛在問題—— 所有組織都應將安全性置於首要任務，與供應商密切計畫合作，將安全風險降到可接受的標準之內，

伺服器停機時間和應用程式不可用的每一分每一秒，都會對業務營運、員工生產力和財務收入，造成負面衝擊與影響。

在 ITIC 2021 年全球伺服器硬體和伺服器作業系統可靠性調查中，IBM Z 大型機、IBM Power Systems、聯想 ThinkSystem、華為 KunLun 和 HPE Integrity Superdome 伺服器（依此順序），持續鞏固最可靠伺服器硬體產品的領先地位。 IBM Z 企業級平台在為超過 93% 的企業使用者，提供了 6 個和 7 個 9（99.9999% 和 99.99999%）的容錯可靠性，獨樹一幟的卓越表現， 除了超級計算機和高可用性 (HA) 硬體之外，沒有任何伺服器平台能夠達到 Z 級別的可靠性、可用性及近乎完美的執行時間和安全性。

十分之九的受訪者肯定 IBM Power Systems 和聯想 ThinkSystem 解決方案，在可靠性和可用性方面均獲得了五個甚至是六個 9（99.999% 和 99.9999%）， 與效能最差的白牌伺服器相比，IBM Power Systems 和聯想 ThinkSystem 平台的可靠性高出 30 倍，成本效益和經濟性也高出 36 倍。

另個顯著的成就中，IBM 和聯想在每個可靠性和可用性類別，都獲得了第一或第二名，或在調查中的每個執行時間、安全性或可管理性指標中並列第一或第二。

可靠性是流動變化的，並非永遠固定， 沒有伺服器，更沒有硬碟、記憶體或 CPU、作業系統、應用程式、裝置或連接機制，能不受固有問題或故障的影響。

伺服器是網路基礎架構和延伸的網路生態系統，賴以存在的重要基石， 當伺服器故障，資料存取就會被拒絕、 業務停止營運、 生產力與 收入受到影響。 如今，約有 88% 的公司要求伺服器硬體、作業系統和主要業務應用程式，具有至少 99.99% 的可靠性，以確保生產力並提供不間斷的資料存取， 高可靠性和可用性還可以保護公司的日常營運、資料資產和智慧財產權 (IP)，以及員工的個人資訊、業務流程和收入流。

安全、人為錯誤和一般使用者，是構成了可能破壞伺服器、作業系統和應用程式可靠性和可用性的最大威脅，

尤其在沒人知道 COVID-19 疫情會持續多久之下的數年之間。 甚至當疫情趨緩後，負面影響和衝擊可能仍會持續，在安全和資料外洩威脅方面更要注意。

新常態是：有組織性的駭客仍然存在， 他們繼續利用疫情大流行來惡意探索安全漏洞，抓住每一個機會來竊取公司、員工資料資產，藉以獲取利潤和勒索。

在 COVID-19 疫情期間的遠距辦公和學習時，伺服器可靠性、不間斷的資料和應用程式存取和安全性，始終必要， 伺服器停機時間和應用程式不可用的每一分每一秒，都會對業務營運、員工生產力和財務收入，造成負面衝擊與影響。

現在，很大一部分的企業伺服器和應用程式，駐留在虛擬化雲環境和網路邊緣， 自疫情大流行以來，企業將員工轉為遠距辦公、學校也採用了遠距學習， 這給組織和過度擴展的 IT 和安全管理員，帶來了更大的壓力，需要確保所有資料資產的執行時間和可用性。

安全性極其重要。 伺服器的供應商必須持續加強嵌入式伺服器的安全性，在發現缺失時快速修正和補強，並與客戶合作提供規範性的指導； 企業還必須承擔責任，確保整個伺服器和網路基礎架構，以及資料中心和雲中的關鍵業務應用程式的可靠性和安全性； 公司得為**所有員工**（尤其遠距員工）實施和執行強而有力的安全政策和程序，這一點不容小覷。 可靠性和安全性是網路基礎架構的核心基本要素， 兩者都是確保不間斷日常營運、安全資料存取和保護收入流所必需的指標。

ITIC 的 2021 全球伺服器硬體，伺服器作業系統安全調查報告，強調需要對**全部**組織，無論規模大小和垂直產業如何，所有組織都需要積極主動地不斷努力識別和挫敗日益複雜和有針對性的網路攻擊。

這代表需要實施全面適當的安全性措施。 為**所有公司員工**（從高階主管到約聘員工和實習生）制定和執行強而有力的電腦安全政策和程序勢在必行。 企業必須為安全產品分配足夠的預算，並投入必要的時間和適當的內部和外部第三方資源，為一般使用者、IT 管理者和安全專業人員提供安全工具和安全培訓。

沒有 100% 萬無一失的安全性。 然而，多層安全性防禦，透過帶動漏洞測試和安全意識培訓，可以阻止資料外洩和勒索軟體駭客侵入的數量，並將風險降低到可接受的標準之內。

Cisco、HPE 和華為的關鍵任務系統也表現出色，自 COVID-19 疫情大流行以來，可靠性沒有出現明顯的下降， 基於核心硬體的固有穩健，Cisco、HPE 和華為伺服器的可靠性可比擬 IBM 和聯想的卓越，

Cisco UCS 伺服器在 ITIC 最新的 2021 年全球伺服器硬體、伺服器作業系統可靠性調查年中更新中，保持可靠性的優勢， 自 2019 年以來，Cisco UCS 伺服器回報的停機時間已

從之前調查的 4.1 分鐘，下降到每台伺服器/每年 2.3 分鐘， 這點很重要， Cisco UCS 伺服器的很大一部分部署在網路邊緣，長期以來被認為是生態系統中最脆弱的攻擊點之一。

所有供應商都不能滿足於現狀， 尤其全球伺服器硬體市場競爭激烈， 持續是一個買方市場。 部分中小企業，根據價格做出採購決策，但大多數的企業選擇購買更強大的硬體，配備嵌入式安全、高級管理、AI 和大數據分析功能。

調查顯示，企業非常重視廠商的售後技術服務和支援， 需要供應商在出現問題時，迅速採取行動。 供應商應就系統配置和產品生命週期，為客戶提供切合實際的建議和規範性指導，以實現並保持最佳效能和可用性。

ITIC 認為供應商也有責任及時提供修補、修正和更新，並儘其所能通知客戶任何可能影響效能的已知不相容問題， 在出現問題或延遲交付更換零件時，坦誠告知。

建議

沒有伺服器平台、伺服器作業系統或商業應用程式，能夠提供萬無一失的安全性， 而 IBM、聯想、華為、HPE 和 Cisco 這些最可靠的伺服器平台，也盡其所能提供了最高層級的固有安全性， 讓客戶能夠實現最大規模經濟並保護敏感的 IP 和資料資產。 安全性是一個 50/50 的提議， 即使供應商提供了強大的安全性，但企業有責任維護伺服器和總體網路基礎架構的可靠性。 ITIC 強烈建議企業：

- **通盤考量。** 知道你的網路上有什麼， 這代表了編目***全部***伺服器、關鍵主要業務線的應用程式、整個網路生態系統內的網路裝置（如防火牆、路由器），其中網路

生態系統包括資料中心、遠端辦公室、公有雲、私有雲和混合雲、物聯網裝置和網路邊緣等。

- **適當容量的伺服器硬體。** 伺服器硬體必須足夠強大，以適應當前的、預期增加的工作負載和更大的應用程式。
- **定期更新伺服器硬體。** 這代表著***基於最新的需求***保持最新的必要修補、更新和安全修正程式，保持系統性能良好，並實現最佳系統效能。
- **更新軟體。** 永遠不要在服務器操作系統和基於服務器的關鍵應用程式上，落後兩個以上的版本。
- **實施強有力的安全性政策和程序。** 各種規模和細分市場產業的企業與公司，都必須構建公司範圍的安全政策和程序， 並透過書面副本和電子郵件，將它們傳達給所有員工。 電腦安全政策應是整體公司的指導方針之一，並且應包含對第一次、第二次和第三次違規的具體規定和懲處， 也建議企業讓所有員工參加強制性的電腦安全培訓。
- **密切監控服務水準協議 (SLA)。** 請密切注意服務水準協定合約，以確保您公司的硬體、軟體供應商、雲端供應商滿足或優於 SLA 的條款，以提供約定的可靠性層次。
- **進行安全漏洞測試。** 鑑於所有類型的安全駭客和資料外洩（如勒索軟體、網路釣魚攻擊和 CEO 詐騙等）持續激增，所有企業每年都應該根據需要，進行至少一次的漏洞測試， ITIC 會建議企業與獨立第三方專家一起合作測試。
- **制定控管和補救計畫。** 有一個補救和控管計劃，可以防止您的公司被駭客入侵，指定發生資料外洩或網路中斷時的負責人等級， 控管和補救計畫應為特定團體和個人，分派和指定特定任務， 確保計畫還包括全部供應商、協力廠商和服務供應商相關的聯絡資訊。

- **培訓和認證安全和 IT 管理者。** 確保安全和 IT 專業人員得到足夠的訓練，並具備必要的安全性認證。
- **培訓一般使用者。** 確保一般使用者以及約聘員工、臨時員工，針對最新電子郵件和網路釣魚詐騙以及勒索軟體威脅，接受足夠的安全意識培訓。

調查方法

ITIC 的 *2021 年全球伺服器硬體安全可靠性調查*，從 2021 年 1 月到 2021 年 6 月中旬，對全球 1000 多家公司的高階主管和 IT 管理員進行調查。 獨立的網路意見調查包括多個選項問題和一個論文問題。 為保持客觀性，ITIC 未接受任何供應商的贊助。 沒有任何接受調查的參與者獲得任何報酬。 ITIC 分析師還進行了二十幾個第一人稱客戶訪談，以獲得寶貴的傳聞資料，並獲得有關安全漏洞和資料外洩對企業伺服器和網路基礎架構可靠性的影響和牽連影響的更深入見解和情境脈絡知識。 受訪者包括高階主管、IT 和安全管理者和一般使用者。 ITIC 採用身份驗證和追蹤機制，來防止篡改並禁止同一方進行多次回應。

調查人口統計資料

ITIC 對 28 個垂直市場的 1,100 家各種規模的公司進行了調查。 各種規模的公司都有很好的代表。 受訪者來自員工少於 50 人的中小型企業 (SMB) 到員工超過 100,000 人的跨國企業。

所有市場部門的代表均相同：擁有 1 到 100 名員工的中小型企業佔受訪者的 24%。 擁有 101 到 1,000 名員工的小型和中型企業 (SME) 佔參與者的 28%。 其餘 43% 的受訪者來自擁有 1,001 至 100,000 名員工的大型企業。 調查受訪者來自 49 個不同的垂直市場。 約 61% 的受訪者來自北美地區；39% 是來自歐洲、亞洲、澳大利亞、紐西蘭、中/南美洲和非洲的 22 個國家的國際客戶。

附錄

本節提供指向本報告中引用各種 ITIC 統計資料的鏈結。

ITIC 網站和意見調查資料和部落格貼文的網址鏈結：

https://itic-corp.com/blog/2019/11/ibm-lenovo-hpe-and-huawei-servers-maintain-top-reliability-rankings-cisco-makes-big-gains-ibm-lenovo-hardware-up-to-24x-more-reliable-28x-more-economical-vs-least-reliable-white-box-servers/

https://itic-corp.com/blog/2019/11/1678/

https://itic-corp.com/blog/2019/08/itic-poll-human-error-and-security-are-top-issues-negatively-impacting-reliability/

https://itic-corp.com/blog/2019/08/itic-2019-server-reliability-mid-year-update-ibm-z-ibm-power-lenovo-system-x-hpe-integrity-superdome-huawei-kunlun-deliver-highest-uptime/

http://itic-corp.com/blog/2017/07/ibm-z14-mainframe-advances-security-reliability-processing-power/

http://itic-corp.com/blog/2017/06/ibm-lenovo-servers-deliver-top-reliability-cisco-ucs-hpe-integrity-gain/