受信任資料中心和儲存基礎結構

DELL Technologies

intel

受信任資料中心儲存基礎結構

由於業務相近，中端市場公司會面臨許多類似的資料中心儲存基礎結構挑戰，但缺乏相同的資源來解決這些問題。容量、停機時間、資料竊盜和違規等問題，皆會拖慢這些組織在競爭日益激烈的環境下持續創新的能力。它們必須確保重要的資料和 IT 資產隨時可用、耐用、可擴充且受到保護。面對這些充滿挑戰的市場動態，中端市場的組織該如何取得成功？

在獲得優異成功的組織中，我們看到他們展現了明確的組織承諾，將包括儲存基礎結構的受信任資料中心基礎結構放在最優先的位置。圖 1 說明受信任資料中心技術、其改善的營運成果，以及最終所實現之業務成功間的關係。

受信任資料中心最佳實務與技術和業務成果之間的關係。

可從以下方面來衡量資料中心安全性和受信任的最佳實務：

- 更頻繁的基礎結構更新
- 組織承諾確保基礎結構技術安全
- 成功實作安全基礎結構技術

安全且受信任的資料中心能提供更優異的技術成果，例如：

- 較少的服務中斷期間
- 更快速的服務和資料復原
- 減少資料遺失與安全性事件
- 更優秀的法規遵循能力

最終，技術和安全性效能可實現更大的業務成功，包括：

- 進入市場的時間更快
- 改善客戶滿意度
- 提高市場佔有率
- 加快營收成長

資料來源：企業策略集團

受信任資料中心的三大運作支柱：

1.定期更新和汰換資料中心基礎結構

2.致力於部署受信任技術

3.實作這些技術

受信任資料中心儲存技術包含加密等現代資料安全性功能、內嵌韌體安全性功能，以及備份頻率和複寫等資料保護實務。

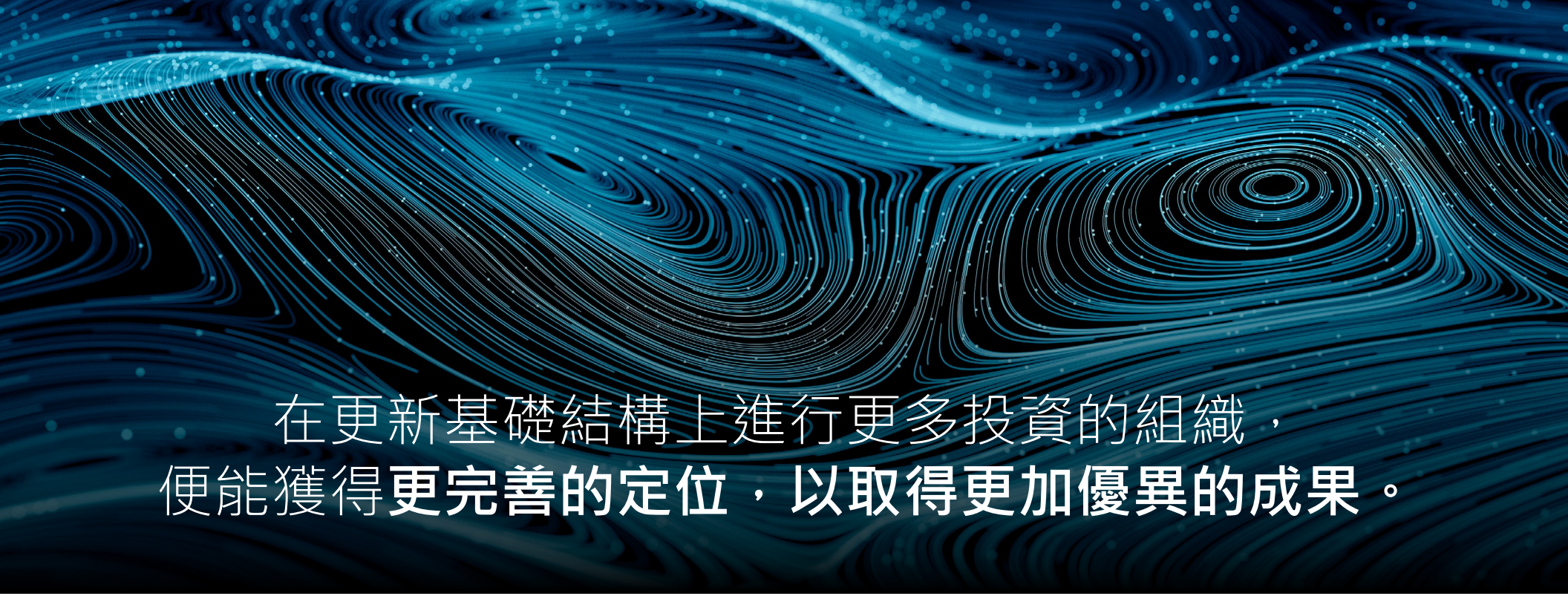
降低威脅資料的風險

中端市場組織必須優先改善 IT 環境的安全性和可靠性，包括儲存基礎結構。透過將安全性漏洞或資料遺失等儲存裝置中斷導致的負面業務影響降至最低，中端市場公司可提升其在市場上競爭並取得成功的能力。

儲存服務對於業務營運至關重要，任何的服務中斷都可能產生有害影響。

- **網路安全風險可能會對組織造成競爭力方面的傷害**
- **服務中斷可能會導致客戶服務中斷**
- **資料遺失會降低生產力，而違規通常會導致直接的財務後果**

安全性策略中應包括規劃基礎結構的更新和汰換。較新的基礎結構通常包含一系列安全性和資料保護功能，舊款解決方案在此方面可能較缺乏。簡而言之，在更新基礎結構上進行更多投資的組織，便能獲得更完善的定位，以取得更加優異的成果。



在更新基礎結構上進行更多投資的組織，便能獲得**更完善的定位，以取得更加優異的成果。**

除了更新基礎結構之外，能掌握成功的組織同時還會致力於其他幾種儲存基礎結構最佳實務，包括：

- **加密敏感性資料，以避免遭竊或損毀**
- **投資韌體內建先進安全性功能的基礎結構解決方案**
- **將敏感性資料複寫到次要儲存系統，以最大化連續運作時間和復原能力。**

成功的組織具備運作更可靠、更有彈性，且難以遭到破解的環境。整體來看，他們發生可能導致資料遺失或遭到入侵的安全性事件數量更少、無法遵循內部治理或法規的實例數量也較低，服務中斷期間也更短，因此能以更快的速度復原。因此我們瞭解，高科技的效能有助於企業在市場上超越競爭對手、提高客戶滿意度，同時提高市場佔有率和營收。

法規遵循是另一個 IT 和業務風險的驅動因素，對表現最佳的組織來說，這也是最重要的承諾。對內部和法規的合規要求可能十分嚴格。對於資源有限的中端市場組織來說，擁有高效率的法規遵循方法至關重要。同時，由於許多中端市場組織在吸收違規的財務處罰方面處於不良地位，因此所採用的方法必須具備優異的效率。

確保儲存基礎結構的可用性

有各式各樣的原因可能會導致儲存裝置服務中斷。天災可能會使某個地區中斷連線、人為錯誤可能導致服務中斷，加上伺服器、儲存裝置或網路元件等系統，都有可能發生故障。若 IT 組織能具備較新的基礎結構，並在高安全性和高可靠性技術解決方案上投入更多資源，就能斬獲優異的成果。

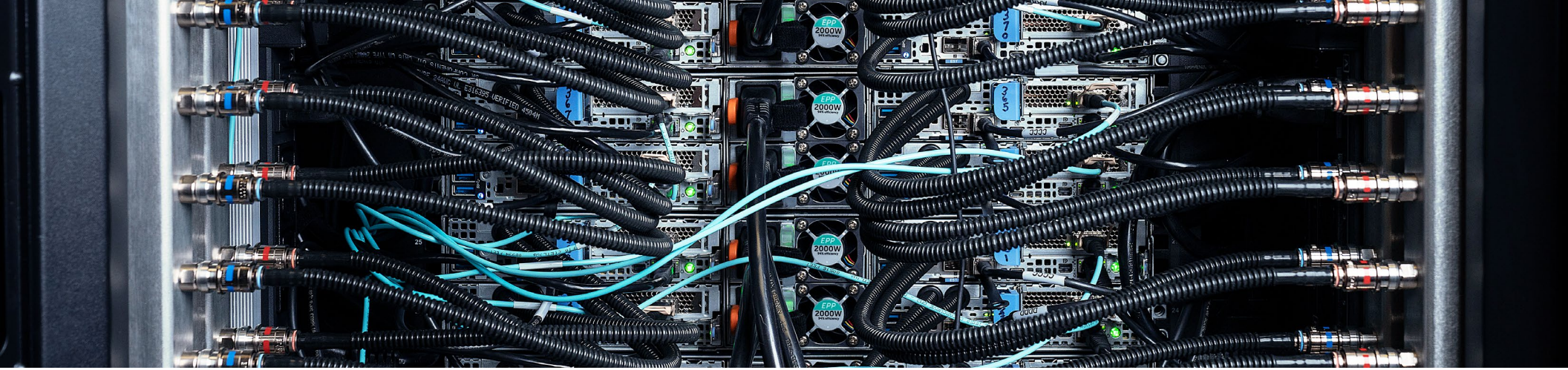
儲存基礎結構的可用性對於當下營運、持續開發和交付新業務服務都極為重要。對依賴這些服務的客戶及使用者而言，儲存裝置服務中斷會造成立即且明顯的影響。對開發團隊的影響則較不明顯。軟體開發實務基本上已從單一的瀑布式方法，轉向靈活的持續性開發和交付模式。儲存服務的損失可能會拖慢開發的步調，並有導致開發工作遺失的風險，需要大量的復原時間。

組織必須**持續保護客戶資料的安全。**

透過受信任資料中心儲存裝置提升商業靈敏性

若組織著重於包括儲存服務的受信任資料中心技術，便能更完善地進行創新、提供新產品，並滿足客戶的期望。隨著消費者和其他企業透過不間斷數位服務獲得優勢，這些期望也變得越來越明顯。對於持續存取業務服務的需求不斷增加，這增加了對高可用性和高擴充性應用程式的壓力。若組織可運行這類應用程式，便能擁有更好的競爭與成長立足點。

僅具有高可用性和擴充能力，不足以滿足現代的數位服務需求。組織必須持續保護客戶資料的安全。資料外洩極為常見，雖然消費者可能預期會發生某些安全性漏洞，但這些攻擊仍會導致財務和聲譽的成本。中端市場企業可以利用受信任資料中心儲存基礎結構，以降低資料外洩、勒索軟體和其他會導致服務中斷的網路安全威脅風險。



組織應努力改善，以符合本文所述的最佳實務，包括：

經常更新伺服器和儲存基礎結構，並使用具備更精密安全性和資料保護功能的解決方案。

優先考慮具備精密「內建」安全性功能的伺服器解決方案。雖然較新的伺服器本身就比舊伺服器更安全，但還是有一些需要看重的特定安全性功能：

- 可檢查所有系統更新是否經過密碼編譯驗證的能力
- 自動鎖定組態設定
- 執行完整系統糾刪的能力

為有效導入最佳實務投入所需的財務和人員資源，確保能實施最佳實務。

沒有任何組織可以忽略安全性威脅而不產生重大的不良影響。受信任資料中心儲存基礎結構模式的最佳實務也大略代表了企業級組織能有效滿足儲存裝置、安全性、法規遵循和作業需求的最佳實務。

深入瞭解 Dell Technologies 如何協助您提升受信任資料中心的成熟度。

DELL Technologies

intel