



Cyberhood 分散式企業平台 國際白皮書

繁體中文版 | Version 3.4

一個分散式平台。一套企業架構。為持續演進而打造。



分散式
基礎架構



資訊保護



企業協作



企業應用



模組化演進

Kinghood Technology

分散式企業解決方案
連結企業、資訊與營運

Version 3.4

文件資訊

文件	Cyberhood 分散式企業平台 — 國際白皮書（繁體中文版）
版本類型	正式出版版
版本	Version 3.4
語言	繁體中文
日期	2026 年 9 月
狀態	Publication Release
發行者	Kinghood Technology

修訂紀錄

版本	日期	說明	狀態
3.3	2026 年 9 月	繁體中文版正式出版 （ Traditional Chinese Publication Release ）	Publication Release
3.4	2026 年 9 月	企業應用整合架構、第 7 章重 構、附錄同步與執行摘要強化	Publication Release

如何閱讀本白皮書

企業主管可先閱讀執行摘要、第 1、2、10 與 11 章。架構師與系統整合商可著重第 2 至 5 章、第 8、9 章及附錄 D。系統管理與技術團隊則可將平台、安全、儲存與部署相關章節作為概念性參考。

適用讀者

- CIO 與 CTO
- 企業架構師與解決方案架構師
- IT 管理者與基礎架構團隊
- 系統整合商與技術合作夥伴
- 開發人員與應用架構師
- 資訊安全與營運專業人員

目錄

執行摘要	4
PART I — 願景	5
企業基礎架構挑戰	6
Cyberhood 分散式企業平台	7
PART II — 核心技術	12
高可用性（High Availability, HA）架構	13
Cyberhood SPAN：分散式受保護資訊架構	18
企業安全架構	26
PART III — 企業平台	30
企業協作平台	31
企業應用生態系統與整合	35
開發者平台與分散式應用框架	42
PART IV — 架構	48
部署模式與參考架構	49
商業價值與企業優勢	61
結論與架構願景	73
技術詞彙	85
參考架構	89
技術重點	92
Cyberhood 架構框架（Cyberhood Architecture Framework, CAF）	94

執行摘要

現代企業需要一個能協調分散式基礎架構、保護資訊、整合專業化應用、支援業務持續性與協作，並為持續應用開發提供基礎的平台。Cyberhood 以統一的分散式企業架構回應這些需求，而非將能力分散於彼此孤立的產品之中。

Cyberhood 結合三項互補的架構責任。分散式架構提供由 Master Nodes、Slave Nodes 與分散式本地節點（Distributed Local Nodes, DLN）構成的營運基礎；Cyberhood SPAN 透過受保護分段、加密、分散配置、門檻重建、裝置層級容錯與保護狀態復原，提供受保護資訊層；企業應用整合則連接專業化應用、交易、訊息、資訊流與企業流程。

在應用層，EIP、ERP、CRM、專案管理、工作流程／電子簽核、通訊與協作及其他企業應用，各自保留專業化業務責任，同時參與協調式企業流程。已實作的整合能力包括 API Integration、Transaction Orchestration、Enterprise Service Bus（ESB）、Message Bus、Automatic Cross-Application Synchronization，以及共享的工作流程機制。

Cyberhood SDK 與 Distributed Application Framework 進一步提供共同的開發基礎。整體形成一個連接基礎架構、受保護資訊、整合服務、專業化應用與協調式企業營運的企業平台，同時保留各業務功能與部署環境應有的責任邊界。

平台觀點

- 分散式基礎架構與高可用性 — 協調分散式資源、負載平衡、故障隔離、重新分配、復原與容量恢復。
- 共同平台服務 — 共享身分、授權、資訊管理、通訊、協作、管理與安全能力。
- 受保護資訊架構 — Cyberhood SPAN 將邏輯企業資訊與個別儲存資源的依賴關係分離。
- 企業整合服務 — API Integration、Transaction Orchestration、ESB、Message Bus 與 Automatic Cross-Application Synchronization。
- 企業流程整合 — 工作流程／電子簽核協調跨應用流程、組織授權、內部稽核、內部控制與後續處理。
- 專業化應用與擴充能力 — EIP、ERP、CRM、專案管理、協作服務、Cyberhood SDK 與 Distributed Application Framework 共同運作於共享架構中。

One Distributed Platform — 分散式架構、受保護資訊、企業整合、專業化應用與協調式企業營運。

PART I — 願景

企業基礎架構挑戰

執行概述

企業 IT 環境必須在可用性、安全性、可擴充性、資訊保護與協作之間取得平衡，同時因應連接分散式使用者與系統日益增加的需求。Cyberhood 平台的定位是整合這些需求，而非僅提供單一軟體功能。

獨立系統的限制

企業經常分別使用不同產品處理儲存、通訊、工作流程、客戶管理、企業資源規劃與應用開發。彼此分離的系統可能造成重複管理、資訊分散，以及不一致的營運模式。

Cyberhood 所提出的架構方向，是提供一個共同的分散式基礎，使多種企業服務能在其上運作。

分散式營運環境

現代企業可能跨越總部、分公司、私有基礎架構及不同地理位置營運。分散式架構提供資源協調的模式，同時支援在地部署與集中式管理。

設計目標

- 可用性與韌性
- 可擴充的基礎架構成長
- 受保護資訊存取
- 整合式協作
- 企業應用支援
- 可擴充的開發能力

重點摘要

- 企業基礎架構日益成為架構層級的問題，而非單一產品可以解決的問題。
- 共同平台可降低不同服務之間的碎片化。
- 分散式設計為多據點營運與未來成長提供基礎。

摘要

企業 IT 環境必須在可用性、安全性、可擴充性、資訊保護與協作之間取得平衡，同時因應連接分散式使用者與系統日益增加的需求。Cyberhood 平台的定位是整合這些需求，而非僅提供單一軟體功能。

第 2 章

Cyberhood 分散式企業平台

分散式企業運算的統一架構

執行概述

現代企業環境正日益走向分散式運作。使用者、資訊、業務流程、應用程式與基礎架構，現今可能分布於總部、分公司、遠端據點、行動裝置以及與雲端連接的環境中。

Cyberhood 以分散式企業平台架構回應此一環境。Cyberhood 並非將儲存、通訊、協作、工作流程、安全、企業應用與應用程式開發視為彼此孤立的技術環境，而是提供一個將這些能力連結起來的共同架構基礎。

其目標不只是提供更多軟體功能，而是建立一個協調一致的平台，使多種企業能力能在一致的架構環境中運作。

2.1 從獨立產品走向整合平台

傳統企業環境往往隨著個別產品的導入而逐步成長。檔案管理、訊息傳遞、工作流程、客戶管理、資源規劃與應用程式開發，可能各自在不同的基礎架構與管理模式上運作。

這可能造成身分管理分散、資訊重複、安全控制不一致、應用整合困難，以及營運複雜度持續增加。因此，架構上的核心問題成為：應由哪些共同基礎架構與平台服務來支援整體企業環境？

Cyberhood 從平台觀點處理這項挑戰。各應用程式仍可服務不同的業務目的，同時運作於共享的架構基礎之上。

2.2 Cyberhood 平台概念

Cyberhood 分散式企業平台整合分散式基礎架構、負載平衡、身分與授權、資訊保護、分散式儲存、協作服務、企業應用、管理，以及應用程式開發。

平台採分層架構組織：分散式基礎架構提供底層基礎；安全與受保護資訊服務提供保護；平台服務提供共同能力；協作與資訊服務連結人員與組織知識；企業應用支援營運；而業務服務則創造組織價值。

2.3 以分散式基礎架構作為基礎

Master Nodes、Slave Nodes 與分散式本地節點（Distributed Local Nodes, DLN）在分散式平台中扮演彼此協調的角色。此架構不將所有服務集中於單一巨型環境，而是支援將服務與資源分布於參與的平台基礎架構中。

此分散式基礎可支援運算服務、連線管理、資料分布、應用程式執行、資訊存取、儲存服務及跨地理位置部署。連線、資料與運算的負載平衡，為工作負載分配與漸進式擴充提供架構基礎。

2.4 共同平台服務層

要讓多個應用程式在一致的環境中運作，就需要共同服務。Cyberhood 提供共享能力，包括身分驗證、授權、資訊索引、工作流程、訊息傳遞、管理、分散式應用服務及 SDK 整合。

這些服務可在身分管理、存取控制、資訊探索、應用整合、管理及未來擴充等面向提供架構一致性。

2.5 以身分作為平台基礎

使用者、應用程式、組織角色與資訊存取權限，都依賴可識別的實體。在 Cyberhood 架構中，身分驗證與授權提供存取平台資源的基礎服務。

此共同模型可支援檔案、共享工作空間、協作服務、企業應用、分散式應用服務及管理功能。

2.6 將資訊視為共享的企業資源

Cyberhood 將檔案管理、分享、工作空間組織、版本控制、全文檢索及跨平台存取，整合於更廣泛的平台架構中。

企業資訊生命週期可理解為：建立 → 儲存 → 分享 → 協作 → 版本管理 → 搜尋 → 保護。此流程將協作、資訊探索與保護連結為共同資訊架構的一部分。

2.7 跨層式安全架構

安全機制橫跨整體架構，涵蓋身分、驗證、授權、安全通訊、主機保護、惡意程式偵測及受保護資訊服務。

此模型並非宣稱任何單一技術可以消除所有風險；相反地，保護機制分布於身分、通訊、基礎架構、資訊與儲存等不同層面。

2.8 Cyberhood SPAN 作為受保護資訊層（Protected Information Layer）

Cyberhood SPAN（Secured & Protected Archive Network）是一種分散式加密檔案系統架構，設計用於結合資訊保護、分散式儲存、容錯、復原及可擴充容量。

SPAN 與資訊管理、檔案服務、協作、安全、分散式基礎架構及災難復原規劃相互連結。因此，它是整體企業資訊架構的一部分，而不是孤立的儲存元件。

2.9 建構於共同基礎上的企業應用

Cyberhood 平台涵蓋 Enterprise Mail、Enterprise Messenger、Workflow、Project Management、CRM、ERP、Calendar 及組織通訊等企業應用領域。

這些應用可與組織身分、授權、資訊服務、工作流程機制、管理、受保護儲存及分散式基礎架構建立共同的架構關係。

2.10 將協作作為原生平台能力

Cyberhood 透過我的空間（My Space）、公共空間（Public Space）、我分享的空間（Sharing With Space）與分享給我的空間（Shared From Space）等概念，將協作與資訊管理整合。

協作可置於更廣泛的架構關係中理解：身分 → 授權 → 工作空間 → 資訊 → 協作 → 保護。

2.11 可延伸的應用程式開發平台

沒有任何組織能預先預測所有未來的應用程式、工作流程、整合需求或業務流程。因此，Cyberhood 提供 Distributed Application Framework 與 SDK。

Cyberhood SDK 為使用者互動、應用程式呈現、伺服器端處理、分散式主機選擇、驗證及平台整合提供基礎。這種可延伸性，正是平台架構與固定功能產品集合之間的重要差異。

2.12 平台擴充性與架構演進

隨著組織成長、使用者增加、資訊量擴大、新應用導入以及更多據點連線，企業需求也會持續改變。

Cyberhood 架構以模組化擴充為設計原則。隨需求演進，可加入額外運算資源、分散式節點、儲存容量、地理位置及應用服務。

2.13 Cyberhood 架構模型

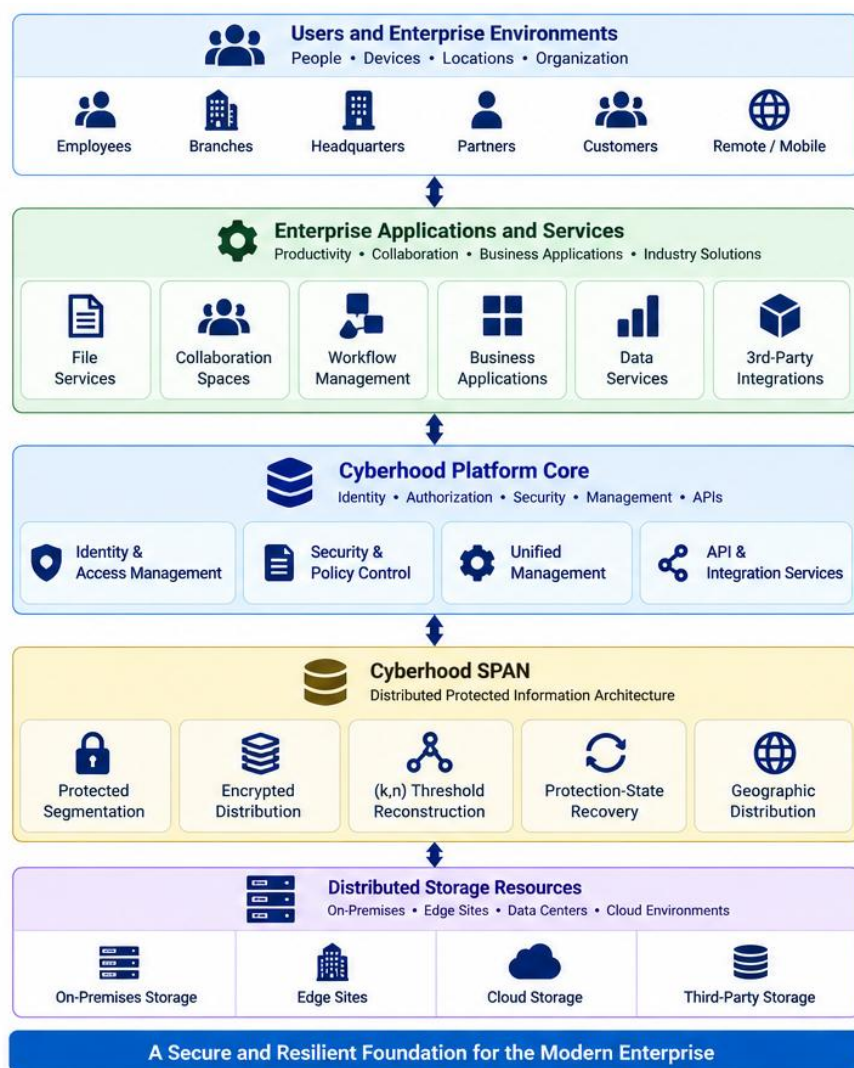


圖 2-1 Cyberhood 架構分層模型

基礎架構提供底層基礎；平台服務提供共同能力；資訊服務連結人員與組織知識；應用程式支援業務營運；Business Services 則創造組織價值。

這項關係構成 Cyberhood 分散式企業平台的核心架構定義。

主要架構原則

Distributed by Design — Cyberhood 以分散式基礎架構為設計核心，而非以單一巨型技術環境為基礎。

Platform Before Product — 應用程式是更廣泛平台架構的一部分，並由共同服務提供支援。

Identity as a Foundation — 身分驗證與授權為平台資源存取提供共同控制機制。

Information as an Enterprise Asset — 資訊管理、分享、搜尋、版本管理、協作與保護，在平台架構中彼此連結。

Security by Architecture — 保護機制橫跨身分、通訊、基礎架構、惡意程式偵測及分散式受保護儲存。

Modular Scalability — 基礎架構、儲存及應用能力可隨組織需求演進而擴充。

Collaboration as a Native Capability — 協作直接與企業資訊、身分、存取控制及平台服務連結。

為未來開發提供擴充性 — Cyberhood SDK 與分散式應用框架（Distributed Application Framework）為持續的應用程式開發與整合提供基礎。

重點摘要

- Cyberhood 是一個統一的分散式企業平台，而非彼此獨立的軟體產品集合。
- 此架構連結分散式基礎架構、平台服務、安全、資訊管理、協作、企業應用及應用程式開發。
- Master Nodes、Slave Nodes 與分散式本地節點（DLN）提供分散式平台部署的概念基礎。
- 連線、資料與運算負載平衡支援可擴充的基礎架構運作。
- 共享平台服務為身分、授權、索引、工作流程、訊息傳遞、管理及應用程式開發提供共同能力。
- Cyberhood SPAN 以分散式加密儲存與容錯機制為基礎，提供受保護資訊層（Protected Information Layer）。
- 企業協作能力將檔案、分享、工作空間、版本控制、搜尋、通訊及受保護資訊管理連結起來。
- 企業應用可運作於共同架構基礎之上，而不必成為彼此孤立的技術環境。
- Cyberhood SDK 提供擴充平台、加入更多分散式應用程式的途徑。
- 此架構透過模組化基礎架構與服務擴充，支援長期演進。

摘要

Cyberhood 代表一種企業運算架構方法，透過共同的分散式平台，將基礎架構、資訊、安全、協作、應用程式及開發服務彼此連結。

平台從分散式基礎架構開始，向上延伸至共享平台服務、受保護資訊管理、企業協作及業務應用。

Cyberhood 不要求每項新服務都建立獨立的技術環境，而是提供一個共同平台，讓既有與未來的應用程式都能在其上運作。

Cyberhood 並非由任何單一應用程式、儲存技術或基礎架構元件所定義；其核心價值在於將這些元素連結起來的架構。

Cyberhood 是一個分散式企業平台，旨在於同一個協調一致的架構環境中，整合基礎架構、資訊、安全、協作、應用程式及未來創新。

企業應用整合作為平台能力

Cyberhood 將分散式企業平台從基礎架構與共同平台服務延伸至整合式企業應用環境。專業化企業應用可參與共享企業流程，同時保留各自業務領域的責任。

平台提供已實作的整合能力，包括 API Integration、Transaction Orchestration、Enterprise Service Bus (ESB)、Message Bus 通訊、Automatic Cross-Application Synchronization，以及共享的工作流程／電子簽核機制。這些能力連接企業環境中的應用、交易、訊息、資訊流與組織流程。

此整合層補充而非取代既有平台架構。分散式基礎架構提供參與資源；平台核心服務提供共同的身分、授權、資訊、通訊、協作、管理與安全關係；企業整合服務連接專業化應用；Cyberhood SPAN 則在採用 SPAN 保護的資訊範圍內提供受保護資訊架構。

分散式基礎架構 → 平台核心服務 → 企業整合服務 → 企業應用 → 業務服務

專業化應用 — 共享整合服務 — 一個分散式企業平台

PART II — 核心技術

高可用性（High Availability, HA）架構

為分散式企業環境中的持續運作而設計

執行概述

企業系統即使在個別基礎架構元件發生故障時，仍應維持可用。

硬體故障、儲存問題、網路中斷、軟體異常、服務過載及地理區域事件，都是企業運算環境中的現實。因此，高可用性不應僅被理解為部署備援硬體。

具韌性的企業架構必須回答更廣泛的問題：當某個元件故障時會發生什麼情況？平台如何持續運作，或如何從故障中復原？

Cyberhood 透過分散式架構模型實現高可用性。相較於完全依賴單一集中式伺服器或儲存系統，此架構支援將運算、連線、資料與資訊資源分散至多個參與節點。

其目標是降低對個別元件不必要的依賴，並為服務持續性、容錯、工作負載分配、基礎架構擴充性、復原能力及地理分散部署建立架構基礎。

因此，高可用性並非獨立功能，而是 Cyberhood 分散式企業平台整體架構的一部分。

3.1 從元件可用性到服務持續性

傳統對可用性的討論通常聚焦於個別元件：伺服器是否正常？儲存系統是否可用？網路連線是否正常？應用程式程序是否正在執行？

這些問題固然重要，但不足以完整描述企業可用性。系統中的硬體可能仍正常運作，但關鍵服務卻不可用；反之，個別元件可能發生故障，而整體服務仍可透過其他可用資源持續運作。

因此，Cyberhood 將「元件可用性（Component Availability）」與「服務持續性（Service Continuity）」加以區分。此架構的目標並非防止每一次個別故障。任何基礎架構都無法保證所有元件永遠持續運作。真正的目標，是降低個別故障對企業所使用服務的影響。

這種以故障為導向的觀點，構成 Cyberhood 高可用性模型的基礎。

3.2 分散式可用性架構

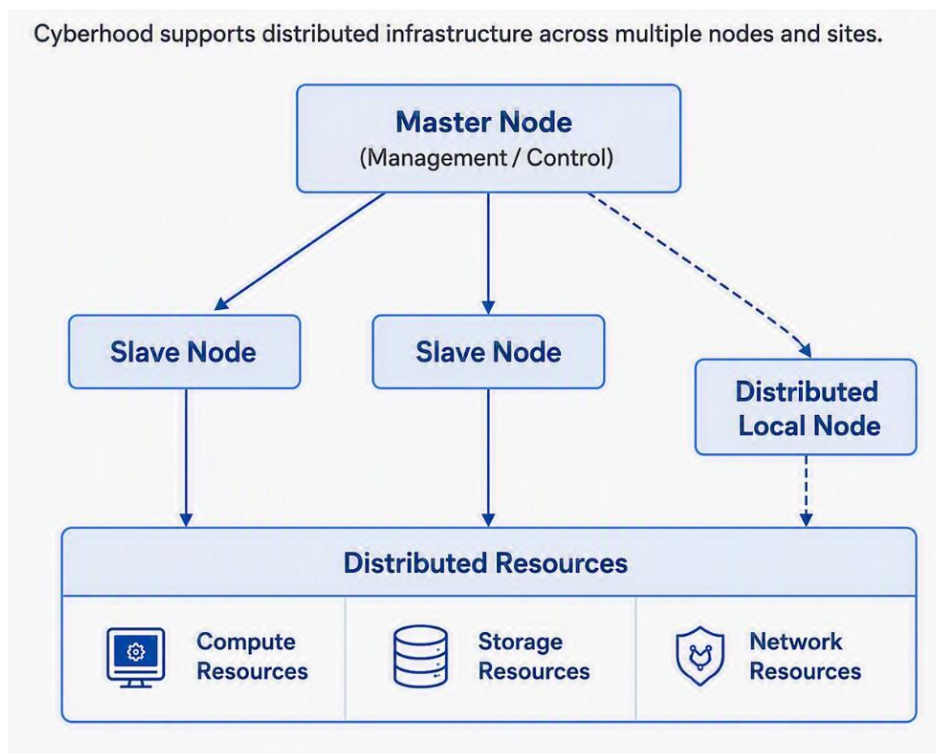


圖 3-1 — 分散式基礎架構參考模型

Cyberhood 平台以分散式基礎架構為核心，包含數種參與節點角色：Master Node、Slave Node，以及分散式本地節點（Distributed Local Node, DLN）。這些角色提供分散平台資源與服務的架構基礎。此模型的目的不只是增加伺服器數量，而是建立一個可讓服務與工作負載分散於可用基礎架構資源之上的環境。

依平台部署與服務設計而定，分散式資源可支援連線處理、應用服務、運算工作負載、資料作業、資訊存取及儲存功能。

因此，分散式架構提供了上層高可用性機制得以運作的結構性基礎。

3.3 消除不必要的單點依賴

當某一個元件的失效會導致整項服務中斷時，即形成單點故障。

分散式架構透過提供替代資源，降低此類依賴；前提是服務設計支援工作負載分配或復原。此原則可應用於運算資源、應用服務、網路連線、儲存資源及不同地理位置。

因此，降低不必要的單點依賴，是高可用性的基本原則。

3.4 故障偵測與資源隔離

高可用性要求平台能辨識參與資源何時不再依預期運作。故障偵測之所以重要，是因為當有替代資源可用時，異常資源不應繼續接收工作負載。資源隔離則可避免故障或不健康的元件對平台其他部分造成不必要的影響。資源被隔離後，架構可依服務設計及可用基礎架構支援選擇替代資源。

這形成從「辨識故障」到「控制故障影響」，最終達到「服務持續性」的轉換路徑。

3.5 連線負載平衡

連線可用性是分散式企業平台的重要面向之一。當使用者或應用程式連接服務時，只要有分散式資源可用，架構就應避免將所有連線活動集中於單一基礎架構元件。

Cyberhood 在其分散式架構中納入連線負載平衡概念。連線分配可降低連線工作負載的集中程度、改善參與資源的利用率、提高基礎架構擴充彈性，並降低對單一連線處理資源的依賴。

若某個參與資源變得不可用，連線管理可依部署架構支援使用其餘可用資源。

3.6 資料負載平衡

企業平台也必須管理資訊與資料處理工作負載的分配。隨著使用者、應用程式與資訊資源增加，集中式系統的需求也會提高。

因此，Cyberhood 將資料負載平衡概念納入其分散式架構。其目標是提供分配資料相關工作負載的架構基礎，而不是將所有處理集中於單一資源。

此模型可支援擴充性、工作負載分配、資源利用及基礎架構擴充，同時與 Cyberhood SPAN 等受保護資訊服務建立架構關係。

3.7 運算負載平衡

應用程式的處理需求並非固定不變。更多使用者、更多應用程式、更高交易量、更多資訊處理及擴大的業務營運，都可能增加運算需求。

Cyberhood 納入運算負載平衡概念，使工作負載可分配至可用的運算資源。這帶來兩項重要架構效益：工作負載可分散而非集中；當容量需求增加時，也可視需要加入額外運算資源。

因此，分散式架構不僅可在故障情況下提升營運彈性，也能在需求增加期間提供更大的調度空間。

3.8 故障情境模型

情境 1 — 個別節點故障

當個別參與節點變得不可用時，架構目標是避免該故障不必要地影響整體服務。依應用程式的部署模型，可用資源仍可持續提供服務。

情境 2 — 運算資源故障

運算資源可能發生硬體異常、作業系統故障、應用程式程序失效或資源耗盡。在應用程式支援工作負載重新分配的情況下，分散式運算架構可提供替代處理資源，以降低單一運算故障對整體平台的影響。

情境 3 — 儲存資源故障

儲存故障可能造成重大影響，因為企業服務仰賴資訊的可用性與完整性。Cyberhood 透過受保護資訊架構與 Cyberhood SPAN 處理此關係。分散式加密儲存模型旨在為受保護資訊提供容錯與復原機制。

情境 4 — 網路或連線故障

網路中斷可能使使用者、服務或基礎架構資源彼此隔離。分散式部署提供讓服務跨多個參與位置或網路路徑運作的架構可能性；實際行為則取決於部署架構、網路設計及應用程式設定。

情境 5 — 服務故障

即使底層硬體仍正常運作，服務本身仍可能不可用。因此，服務層級的監控與復原是可用性架構中的重要概念。架構目標是偵測服務故障、在適當情況下隔離異常資源，並利用可用資源恢復服務。

情境 6 — 地理區域或站點故障

局部事件可能影響整個基礎架構位置，包括電力中斷、網路故障、設施事件、天然災害或長時間基礎架構中斷。地理分散式架構可降低單一地點事件自動導致所有平台資源同時喪失的風險，進一步增加韌性。

3.9 高可用性與 Cyberhood SPAN

基礎架構可用性與資訊可用性密切相關。如果服務所需資訊無法存取或復原，即使應用服務本身持續運作，也無法提供有意義的持續性。

因此，Cyberhood SPAN 是整體可用性架構的重要組成。SPAN 以分散式儲存、加密、容錯、復原及容量擴充為基礎，提供受保護資訊模型。

因此，高可用性不僅是讓應用程式程序維持運作，也包括維持或恢復企業服務所需資訊之存取能力。

3.10 地理分散與災難復原（Disaster Recovery, DR）

高可用性與災難復原彼此相關，但處理的是不同的營運目標。

高可用性主要著重於在營運故障期間維持服務持續性；災難復原則著重於重大中斷後恢復服務與資訊。

Cyberhood 分散式架構透過分散式基礎架構與受保護資訊服務，提供可同時支援這兩項目標的基礎。

3.11 將擴充性視為可用性能力

可用性經常只從故障角度討論，但容量不足同樣可能降低服務可用性。服務即使技術上仍在運作，若因過載而無法使用，對使用者而言仍等同於不可用。

Cyberhood 支援透過增加運算資源、分散式節點、儲存容量、平台服務及地理位置進行模組化擴充。這使企業能在容量限制演變成服務中斷之前，因應成長需求。

3.12 營運持續性模型

完整的 Cyberhood 高可用性模型可概括為持續循環：監控 → 偵測 → 隔離 → 重新分配 → 持續服務 → 復原 → 恢復容量 → 監控。

故障不被視為架構之外的例外事件；相反地，此架構預期基礎架構元件可能故障，因此平台必須提供持續運作、復原及恢復能力的相關機制。

關鍵架構原則

故障導向設計 — 架構會考量基礎架構元件變得不可用時應如何處理。

分散式資源 — 運算、連線、資料與資訊服務可分散於參與的基礎架構資源。

降低依賴 — 在服務設計支援替代資源的前提下，架構致力降低對個別元件不必要的依賴。

工作負載分配 — 連線、資料與運算負載平衡概念，提供分散營運需求的基礎。

故障控制 — 應隔離故障或異常資源，以降低其對整體服務環境造成不必要的影響。

服務持續性 — 目標是維持或恢復企業服務，而非只關注個別元件是否仍在運作。

受保護資訊 — Cyberhood SPAN 將高可用性與受保護資訊、分散式儲存、容錯及復原連結起來。

地理韌性 — 分散式部署可支援因應局部基礎架構或站點層級事件的韌性。

模組化擴充 — 可隨組織需求演進加入額外基礎架構資源。

重點摘要

- 高可用性是一種維持服務持續性的架構方法，而不只是部署備援硬體。
- Cyberhood 採用包含 Master Node、Slave Node 與分散式本地節點（DLN）的分散式基礎架構模型。
- 連線、資料與運算工作負載可分配至參與資源。
- 此架構致力降低不必要的單點依賴。
- 故障偵測與資源隔離提供控制基礎架構問題影響範圍的概念性路徑。
- 依部署與服務架構，可利用其他可用資源支援工作負載重新分配。
- 高可用性除了應用程式與基礎架構可用性之外，也必須涵蓋資訊可用性。
- Cyberhood SPAN 提供受保護的分散式資訊層，有助於容錯與復原。
- 地理分散可增加對局部基礎架構或站點層級事件的韌性。
- 擴充性可隨營運需求增加而擴大基礎架構容量，進而支援可用性。
- 災難復原與高可用性處理不同目標，但可在共同的分散式架構中運作。

摘要

Cyberhood 高可用性架構建立在一項原則上：企業服務不應不必要地依賴單一基礎架構元件持續運作。

透過分散式基礎架構、工作負載分配、資源隔離、受保護資訊服務及模組化擴充，此架構為提升服務持續性與復原能力建立基礎。

架構目標並不是宣稱可以消除故障。故障是企業運算環境中可預期的現實；真正的目標，是讓平台能偵測、控制並處理個別故障，而不使其自動演變成整個服務環境的喪失。

因此，Cyberhood 將高可用性視為持續的架構循環：監控 → 偵測 → 隔離 → 重新分配 → 持續運作 → 復原 → 恢復。

此模型將基礎架構韌性與資訊保護、擴充性、地理分散及長期營運持續性連結起來。

Cyberhood SPAN：分散式受保護資訊架構

執行概述

企業資訊保護通常結合儲存備援、備份、加密、存取控制、惡意程式防護與災難復原。每一種機制分別處理資訊可用性、機密性、完整性或可復原性的不同面向。

Cyberhood SPAN（Secured & Protected Archive Network）為受保護企業資訊導入分散式方法。SPAN 會將受保護資訊進行分段、加密、分散、儲存、重建與復原。其保護模型源自 (k,n) 門檻式秘密分享機制（threshold secret sharing scheme）的原理：受保護資訊會被轉換為多個分散式區段，而重建需要達到定義的最少有效區段數量，並具備所需的密碼學資訊。

分段 · 加密 · 分散 · 容錯 · 重建 · 復原

在 Cyberhood 分散式企業平台中，SPAN 作為 Protected Information Layer 運作。其架構目的，是降低邏輯企業資訊對任何單一實體儲存資源的依賴。

4.1 SPAN 架構概述

Cyberhood SPAN 將邏輯企業資訊與用於保護及儲存該資訊的個別實體資源分離。在邏輯層級，使用者與企業服務操作的是檔案與資訊資源；在保護層級，SPAN 將受保護資訊轉換為加密的分散式區段；在實體層級，參與的儲存資源提供承載這些受保護區段的基礎架構。

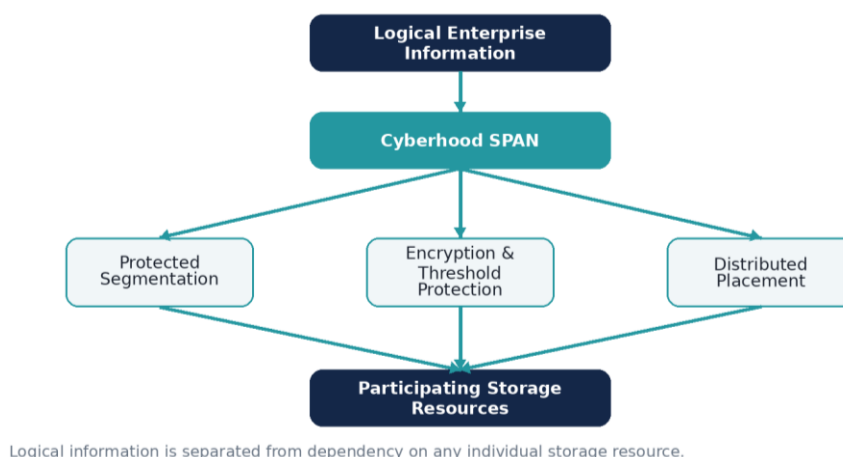


圖 4-1 — Cyberhood SPAN 受保護資訊層（Protected Information Layer）

邏輯資訊與對單一實體儲存資源的依賴相互分離。

4.2 超越傳統備份架構

傳統備份架構通常透過保存額外的完整副本來保護資訊。廣為採用的 3-2-1 備份原則提供了實用的概念參考：保留多份資訊副本、使用一種以上的儲存媒體，並維持地理分離的保護。

SPAN 導入另一種架構模型。受保護資訊不必完全依賴完整副本複製，而可轉換為加密區段並分散至參與的儲存資源。

備份、高可用性、災難復原與 SPAN 處理不同的架構責任，彼此可以並存。SPAN 的主要差異在於「分散式受保護資訊重建」，而非只依賴完整副本複製。

4.3 分散式檔案分段

SPAN 的第一項核心保護作業，是將邏輯企業檔案轉換為多個受保護區段。受保護區段的總數以 n 表示，SPAN 再將這些區段分散至參與的儲存資源。

因此，一個受 SPAN 保護的檔案，是由一組分散式受保護元件所表示，而不是依賴單一儲存資源中的完整可用檔案。

單一受保護區段並不是完整的原始檔案。

4.4 (k,n) 門檻式保護模型

Cyberhood SPAN 採用源自 (k,n) 門檻式秘密分享機制原理的保護模型。在此模型中， n 為受保護區段總數， k 為重建所需的最少有效受保護區段數，且 $k \leq n$ 。

設定的容錯關係為 $f = n - k$ ，其中 f 代表在仍可滿足最低重建門檻的情況下，允許不可用的受保護區段數量。例如，若 $n = 7$ 、 $k = 4$ ，則 $f = 3$ 。在此示例設定中，重建需要 4 個有效受保護區段；最多可有 3 個區段不可用，而剩餘區段數仍不低於重建門檻。

參數	意義	架構角色
n	受保護區段總數	分散式保護集合
k	重建所需的最少有效區段數	重建門檻
$f = n - k$	設定關係可容忍的不可用區段數	容錯條件
受保護區段	加密後的分散式元件	將受保護資訊與個別儲存資源的依賴分離
參與儲存資源	保存受保護元件的資源	分散式保護的實體基礎

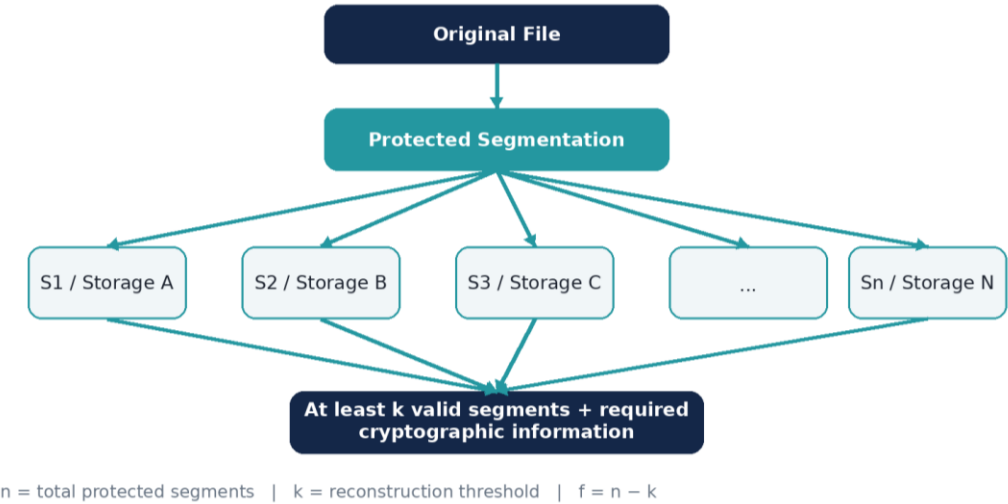


圖 4-2 — (k,n) 門檻式分散保護模型

適當的 k 與 n 值應依保護需求及部署設定決定，而不是採用單一通用常數。

4.5 分散式加密與密碼學關係

僅有分段並不構成完整的 SPAN 保護模型。SPAN 將受保護分段與加密，以及重建所需的密碼學資訊結合。因此，授權重建取決於所需的受保護區段、必要的密碼學資訊，以及授權存取。

單一參與儲存資源本身，並不預期包含重建完整原始資訊所需的全部條件。

分段 → 加密 → 分散 → 授權 → 重建

4.6 裝置層級容錯

傳統磁碟備援通常保護單一儲存設備內的個別磁碟故障。SPAN 則透過將受保護資訊分散於多個參與儲存資源，把保護邊界延伸至單一儲存設備之外。這使單一儲存設備內的「磁碟層級備援」與跨分散式儲存資源的「裝置層級容錯」形成明確區別。

因此，參與的儲存裝置可成為 SPAN 保護架構中的容錯單位。

當某個參與資源不可用時，只要可用有效區段數量仍大於或等於 k ，受保護資訊仍可重建。底層磁碟備援可與 SPAN 的裝置層級保護並存。

4.7 動態容錯設定

SPAN 的保護條件可隨參與資源環境改變而演進。擴充可用儲存資源，可增加受保護區段分配與容錯設定的選擇；因此， n 、 k 與 f 之間的關係可依可用環境及保護需求調整。

增加容量並不會自動提高容錯能力。實際保護條件取決於可用資源、分散設定、重建門檻及保護政策。

基礎架構擴充提供更多保護選項；實際容錯條件由保護政策決定。

4.8 裝置隔離與 Hot-Swap 作業

只要剩餘的保護狀態仍符合設定的重建門檻，SPAN 支援隔離異常的參與儲存資源，並在整體受保護資訊環境持續運作的情況下加入替代或額外資源。

在此架構中，Hot Swap 指的是在不刻意讓整個邏輯受保護資訊環境離線的情況下，隔離、替換或加入參與儲存資源的營運能力；它並不代表特定硬體匯流排層級的熱插拔實作。

偵測 → 隔離 → 持續運作 → 替換／新增 → 恢復保護

4.9 保護狀態復原 (Protection-State Recovery)

容錯處理的是資源不可用期間如何持續運作；保護狀態復原處理的則是之後如何恢復。當不可用資源被隔離或替換後，SPAN 可重新分配受保護資訊，並恢復適當的分散式保護狀態。

因此，SPAN 的復原著重於恢復分散式保護關係，而不只是從另一份備份副本還原單一檔案。

復原的是保護狀態，而不只是單一檔案。

4.10 自動化儲存分配與平衡

隨著資訊成長，以及資源新增、移除、替換或擴充，參與的儲存容量會持續變化。SPAN 納入自動化儲存分配與平衡，使受保護資訊能分散於可用的參與資源。

當資源環境改變時，可重新分配受保護資訊，使新增容量參與更廣泛的 SPAN 環境，並重新平衡儲存利用率。因此，儲存平衡同時支援容量利用與保護狀態管理。

4.11 加密前的惡意程式防護

Cyberhood SPAN 在受保護分段、加密與分散式儲存之前整合 ClamAV 惡意程式檢查。於受保護儲存前進行掃描，可在邏輯檔案被轉換為加密分散式元件之前完成惡意程式檢查。這可降低受感染內容被保存為受保護企業資訊，之後又被重建並散布至其他端點的風險。惡意程式檢查仍只是 Cyberhood 企業安全架構的一部分，不能取代端點安全、身分保護、授權、應用程式安全、網路防護或安全監控。

先檢查，再保護（Inspect Before Protect）。

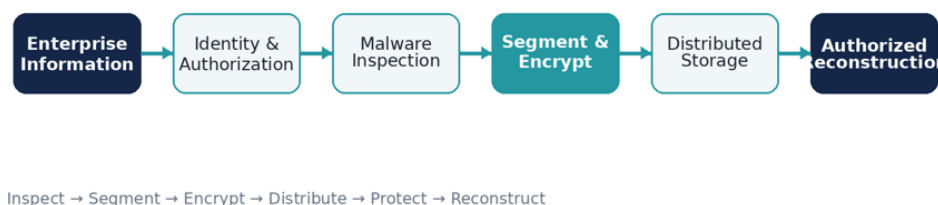


圖 4-3 — SPAN 資訊保護流程

4.12 防範裝置損壞與資訊遺失

實體儲存資源仍可能遭遇硬體故障、斷電、實體損壞、環境事件、網路斷線或管理性隔離。SPAN 透過分散式分段與門檻式重建，降低受保護資訊對單一資源的依賴。

只要設定的重建門檻仍能滿足，即使個別參與資源不可用，受保護資訊仍可保持可重建。SPAN 並不消除實體儲存故障，而是降低受保護資訊對任何單一故障事件的依賴。

裝置故障 ≠ 自動等同資訊遺失

4.13 防範單一裝置遭入侵

分散式受保護資訊會改變單一儲存資源遭入侵時的安全影響。由於 SPAN 資訊經過分段、加密與分散，僅取得一個參與儲存資源本身，並不足以取得完整原始檔案。這可降低資訊機密性對任何單一參與儲存資源的依賴。但這不代表端點、授權帳號、應用程式、管理環境或足夠數量的參與資源遭入侵時，不會影響資訊安全。

單一儲存資源遭入侵，不應等同於完整受保護檔案遭入侵。

4.14 具勒索軟體韌性的資訊架構

對勒索軟體的韌性需要多層安全機制。SPAN 透過分散式受保護分段、加密儲存、門檻式重建、裝置層級分散、授權關係及保護狀態復原，對此韌性提供支援。

此架構可降低單一參與儲存資源遭入侵、損壞、加密或變得不可用時的影響。SPAN 並不代表具備全面的勒索軟體免疫能力；端點遭入侵、憑證竊取、應用程式弱點、管理環境遭入侵、經授權的破壞性操作及其他攻擊途徑，仍屬整體企業安全架構必須處理的責任。

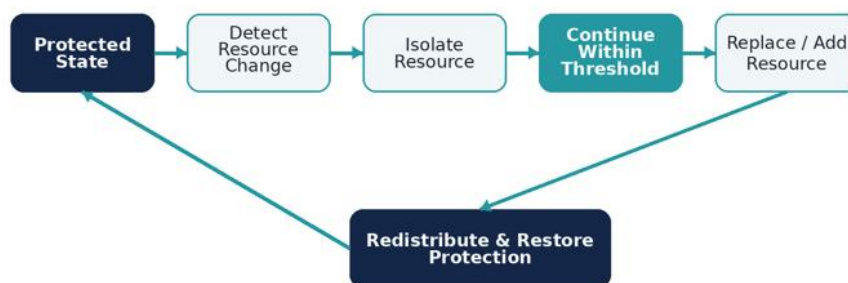
SPAN 強化勒索軟體韌性；但不取代多層企業安全。

4.15 地理分散資訊保護

SPAN 可將受保護資訊元件分散至位於不同網路或地理環境中的參與資源。透過企業網路或 Internet 的點對點通訊，可使受保護資訊的保護邊界延伸至單一實體站點之外。

地理分散可降低所有受保護元件對單一實體位置的依賴。應用程式容錯移轉、Active-Active 服務運作、復原順序、RPO 與 RTO，則取決於更廣泛的部署與復原架構。

地理分散資訊 ≠ 自動地理服務容錯移轉



Recover the protection state, not merely the individual file.

圖 4-4 — SPAN 容錯與保護狀態復原模型

4.16 模組化儲存擴充

SPAN 支援透過加入參與儲存資源進行模組化儲存擴充。新增加的容量可納入分散式環境，並可隨資源設定演進重新分配受保護資訊。傳統 NAS 資源也可在更廣泛的 SPAN 架構中提供儲存容量。

實際可擴充規模仍受基礎架構、網路、軟體、管理、效能及部署條件限制。其架構價值在於模組化成長。

增加資源 → 擴充容量 → 重新評估分配 → 重新平衡保護

4.17 平行資訊存取與串流

重建所需的受保護元件可能位於多個參與資源。因此，SPAN 可在資訊存取過程中支援從分散式儲存資源並行擷取，以及檔案串流傳送。

平行處理並不代表固定的效能倍增。實際效能取決於網路頻寬與延遲、儲存效能、檔案特性、設定的 k 與 n 關係、同時工作負載、重建處理及部署拓撲。

SPAN 為平行受保護資訊擷取與串流提供分散式基礎；實際效能取決於部署條件。

4.18 SPAN 與企業資訊服務

SPAN 位於較上層的 Cyberhood 資訊與協作服務之下，作為受保護資訊基礎。使用者與應用程式操作的是邏輯企業資訊，而不是直接管理分散在實體儲存資源中的個別受保護區段。

Cyberhood 資訊空間透過平台服務與授權，以邏輯資訊環境呈現，而不是直接存取底層個別受保護區段。

邏輯資訊 ≠ 實體儲存位置

企業服務操作資訊；SPAN 管理該資訊的分散式保護。

SPAN 不應被理解為會自動保護每一個 Cyberhood 應用程式產生的所有資料物件。是否使用 SPAN，取決於應用程式設計、平台設定、資訊分類及組織需求。

4.19 SPAN 資訊保護生命週期

SPAN 是受保護資訊的生命週期，而不只是儲存目的地。此生命週期由兩條互補的營運路徑構成。

資訊保護路徑

企業資訊 → 身分與授權 → 惡意程式檢查 → 受保護分段 → 加密 → 分散配置 → 受保護儲存 → 授權擷取 → 門檻式重建 → 企業資訊

保護狀態維護路徑

受保護狀態 → 監控資源環境 → 資源變更／故障 → 辨識與隔離 → 評估剩餘保護狀態 → 在可用容錯條件內持續運作 → 替換／新增資源 → 重新分配受保護區段 → 重新平衡 → 恢復保護條件

第一條路徑保護資訊；第二條路徑維持保護狀態。兩者共同形成：保護資訊 → 維持保護 → 重建資訊。

資訊保護是一個生命週期，而不是一次儲存事件。

4.20 Cyberhood SPAN 架構模型

完整的 SPAN 架構透過 Protected Information Layer，將邏輯企業資訊與分散式實體基礎架構連結起來。

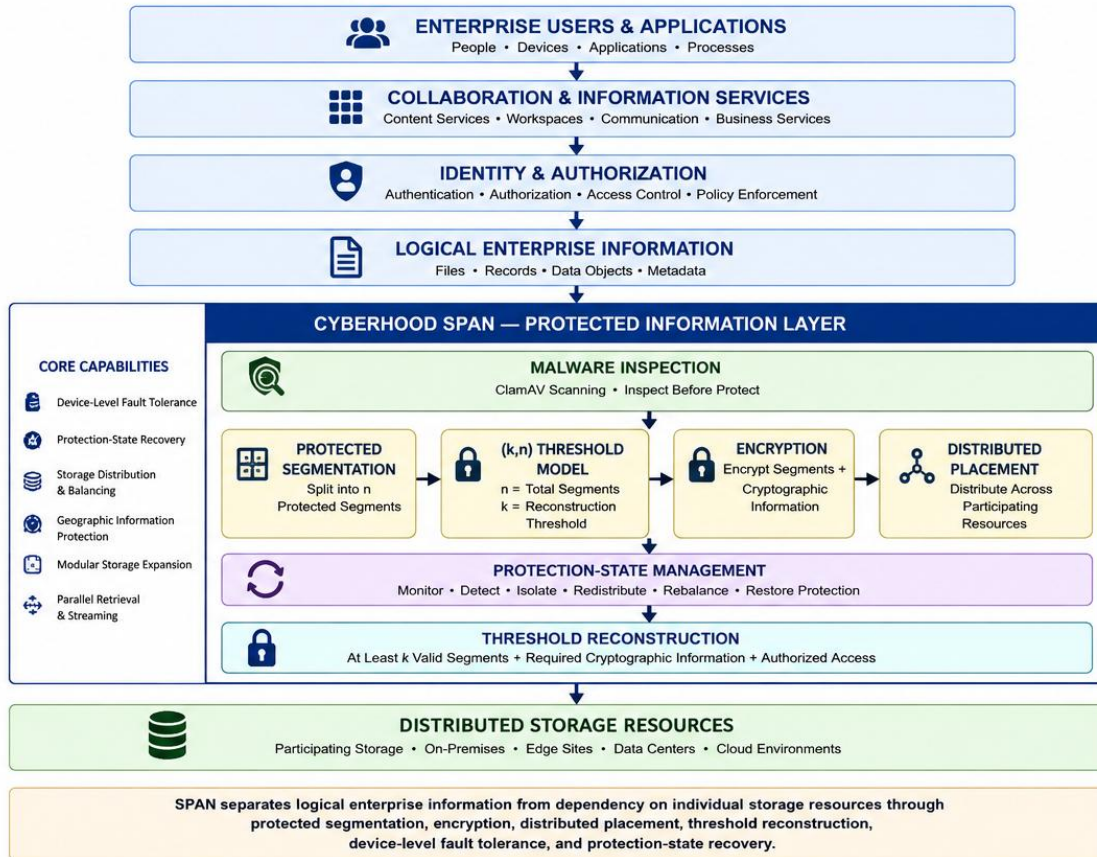


圖 4-5 — Cyberhood SPAN 架構模型

因此，SPAN 不只是加密儲存。其架構結合分段、加密、分散配置、門檻式重建、裝置層級容錯、保護狀態復原、資源重新分配及資訊生命週期管理。

檢查 → 分段 → 加密 → 分散 → 保護 → 監控 → 復原 → 重建

Cyberhood SPAN 是一種分散式受保護資訊架構，透過受保護分段、加密、分散配置、門檻式重建、裝置層級容錯及保護狀態復原，將邏輯企業資訊與對個別儲存資源的依賴分離。

Cyberhood SPAN — Cyberhood 分散式企業平台的受保護資訊層 (Protected Information Layer)

關鍵架構原則

- 資訊以分散式關係受到保護 — 保護建立在受保護元件與參與資源之間，而不是只依賴單一完整實體副本。
- 邏輯資訊與實體儲存分離 — 企業服務操作邏輯資訊，而 SPAN 管理其分散式受保護表示形式。
- 門檻式重建定義可復原性 — k 與 n 的關係決定重建門檻及設定的容錯條件。
- 容錯超越個別磁碟 — SPAN 將保護延伸至跨分散式儲存資源的裝置層級容錯。
- 個別資源故障不會自動等同資訊遺失 — 只要仍有足夠的有效受保護區段，資訊即可維持可重建。
- 保護狀態必須可復原 — 復原包括恢復分散式保護關係，而不只是擷取單一檔案。
- 先檢查，再保護 — 惡意程式檢查先於加密分散式儲存。
- 地理分散延伸保護邊界 — 受保護元件可跨不同位置參與，而不代表自動服務容錯移轉。
- 儲存成長延伸保護架構 — 增加參與資源可擴充容量，而不改變 SPAN 的基本模型。
- 資訊保護是一個生命週期 — 保護持續涵蓋儲存、監控、資源變更、重建、重新分配及保護狀態復原。

重點摘要

Cyberhood SPAN 建立在五項核心資訊保護概念之上：分段 · 加密 · 分散 · 容錯 · 重建。

分段 → 加密 → 分散 → 容錯 → 重建

監控 → 偵測 → 隔離 → 重新分配 → 恢復保護

這些能力共同建立 SPAN 作為 Cyberhood 分散式企業平台的 Protected Information Layer。其差異不只是資訊經過加密或儲存在多個裝置，而是邏輯企業資訊透過分散式關係受到保護，從而降低對任何單一儲存資源的依賴。

摘要

企業資訊保護通常結合儲存備援、備份、加密、惡意程式防護、存取控制、高可用性及災難復原。Cyberhood SPAN 處理的是一項不同的架構責任。

SPAN 不讓受保護企業資訊完全依賴儲存在個別實體儲存資源中的完整檔案，而是將其轉換為分散、加密且可依門檻重建的關係。邏輯企業檔案可被分段並分散至參與儲存資源，而設定的 (k,n) 關係決定重建所需的最少有效受保護區段數，以及相對應的容錯條件。

單一儲存裝置並不等於資訊本身

單一受保護區段並不是完整檔案

單一裝置故障不會自動等同資訊遺失

SPAN 進一步透過裝置層級容錯、資源隔離、保護狀態復原、自動化儲存分配、惡意程式檢查、地理分散資訊保護、模組化擴充及分散式擷取延伸此基礎。這些能力是對企業安全、高可用性、備份及災難復原架構的補充，而不是取代。

SPAN 保護的是企業資訊與其所依賴分散式基礎架構之間的關係。

企業資訊不應只依其儲存位置受到保護，也應透過如何分段、加密、分散、授權、重建及復原來獲得保護。

第 5 章

企業安全架構

執行概述

安全是一項橫跨身分、授權、安全通訊、Independent Firewall 防護、惡意程式防護與受保護資訊儲存的架構能力。Cyberhood 將這些機制整合於整個分散式企業平台，而非將安全視為獨立附加功能。

5.1 安全作為架構原則

企業安全必須保護資訊、通訊、基礎架構、身分，以及對組織資源的存取。Cyberhood 將資訊安全視為整合於分散式平台中的架構能力。

Cyberhood 安全架構結合：

- 安全通訊 + 分散式基礎架構防護 + 系統化資訊保護

這些能力與身分及授權機制共同運作，建立多層式企業安全環境。

5.2 安全網路通訊

通訊安全是分散式企業平台的基本需求。Cyberhood 採用 SSL 等級或更高等級的安全通訊協定，並結合平台加密機制，以保護傳輸中的資訊。

5.3 分散式主機防護

分散式平台包含多個基礎架構節點，因此僅保護網路周界並不足夠。

Cyberhood 為分散式主機提供 Independent Firewall，建立額外的防護邊界，以降低未經授權存取企業資訊與資產的風險。

5.4 系統化資訊保護

企業資訊在整個生命週期中都需要受到保護。Cyberhood 將系統化資料保護與個人化授權結合，建立組織身分、使用者帳號、組織角色、資源權限與資訊存取之間的關係。

5.5 組織身分與帳號管理

Cyberhood 將組織帳號管理納入企業協作環境。個人帳號是資源權限管理的基礎，並可依組織需求對應一個或多個組織角色。

5.6 身分驗證與授權

身分驗證用以確認誰正在要求存取；授權則決定已通過驗證的身分可存取哪些資源。Cyberhood 將個人帳號與資源權限及組織角色連結，以建立對企業資訊的受控存取。

5.7 個人化授權

企業組織具有不同的職責、部門、專案與組織角色。Cyberhood 支援個人化授權，使資訊存取能對應組織角色與使用者帳號。

5.8 橫跨企業資訊服務的安全

安全控制不僅限於檔案儲存。Cyberhood 將資訊保護整合至 Enterprise Mail、Enterprise Messenger、檔案管理、Workflow、Project Management、CRM、ERP 及相關企業服務與應用。

因此，只要企業服務處理或交換資訊，安全機制就應隨資訊而存在。

5.9 檔案存取保護

Cyberhood 的檔案管理環境提供我的空間（My Space）、公共空間（Public Space）、我分享的空間（Sharing With Space）與分享給我的空間（Shared From Space）等不同資訊空間。這些空間結合帳號權限與授權，形成控制資訊存取的結構化模型。

5.10 分散式資訊保護

Cyberhood SPAN 將安全架構延伸至受保護儲存。SPAN 是分散式加密檔案系統，結合資訊保護、分散式儲存、容錯、復原與可擴充容量。

存取控制決定誰可以存取資訊；加密保護分散式儲存架構中的資訊；分散配置與容錯則降低對個別儲存資源不必要的依賴。

5.11 惡意程式防護

Cyberhood 將 Clam AntiVirus（ClamAV）掃描整合至資訊保護架構。檔案在加密與儲存前先進行病毒掃描，使資訊進入受保護儲存之前即具備一層惡意程式偵測。

5.12 入侵與勒索軟體防護

Cyberhood SPAN 將高度加密的分散式儲存與多個獨立存取屏障結合。若要直接存取實際檔案，必須通過多個彼此獨立的存取控制層。

單一裝置遭入侵本身並不足以取得原始檔案內容。使用者電腦上的勒索軟體若未取得合法身分驗證，無法直接控制 SPAN 中的檔案。

這些機制應被理解為多層式架構防護，而不是對所有安全事件的絕對保證。

5.13 安全與容錯

安全與可用性密切相關。儲存資源可能因設備故障、實體損壞或惡意活動而無法使用。

Cyberhood SPAN 透過分散式儲存與容錯機制處理此關係。損壞或不可用的設備可被隔離，並在設備替換或執行復原程序後恢復設定的保護條件。

5.14 安全與分散式架構

Cyberhood 的安全模型與其分散式架構密不可分。平台將基礎架構、服務、資訊、儲存、安全邊界與存取控制分布於多個架構層次。

5.15 安全與企業協作

企業協作會持續產生資訊交換。

Cyberhood 在同一平台環境中提供私人訊息、檔案分享、專案協作、工作流程與企業應用。

Cyberhood Messenger 架構提供一對一與群組通訊，並支援文字、圖片、影片及檔案交換。

企業導向的通訊，使組織能對企業環境中的人員、通訊管道與交換資訊保有更高程度的管理能力。

這形成一項架構優勢：

- 通訊、協作、身分、授權與資訊保護可在共同的企業環境中運作。

5.16 安全稽核與管理控制

安全不僅需要預防，也需要可視性與管理監督。Cyberhood 企業服務可保留活動紀錄，以支援稽核或監督用途，而對這些資訊的存取仍由系統控制。

因此，安全管理涵蓋身分、存取控制、資訊保護、活動紀錄與管理監督。

5.17 多層式企業安全模型



圖 5-1 — 安全架構模型

Cyberhood 安全架構可表示為多層式模型：企業應用與協作位於身分與授權、惡意程式防護、SPAN 加密儲存、分散式基礎架構、安全通訊及 Independent Firewall 防護之上，並與這些能力形成架構關係。

關鍵架構原則

- 多層防禦 — 企業安全由多種互補的防護機制共同建立。
- 以身分為核心的存取 — 資源存取與使用者帳號及組織角色相關聯。
- 分散式防護 — 安全機制延伸至分散式基礎架構，而非僅依賴中央網路周界。
- 受保護資訊 — 企業資訊透過授權、加密、分散式儲存及相關控制受到保護。
- 儲存前惡意程式檢查 — 檔案可在進入受保護加密儲存前先進行掃描。
- 存取層分離 — 受保護資訊透過身分驗證、授權與分散式儲存架構，與端點直接存取分離。
- 具容錯能力的保護 — 資訊保護納入容錯與復原機制。
- 管理可視性 — 活動紀錄可支援企業服務中的稽核與監督。

重點摘要

- Cyberhood 將安全視為架構能力，而不是單一產品功能。
- 安全網路通訊是基本的安全層。
- 分散式主機可透過 Independent Firewall 受到保護。
- 組織帳號提供權限管理的基礎。
- 使用者帳號可對應一個或多個組織角色。
- 授權將組織身分與資源存取連結。
- Cyberhood SPAN 為安全架構加入加密分散式儲存。
- 檔案會在加密與儲存之前進行惡意程式掃描。
- 分散式加密儲存可在遭入侵端點與受保護資訊之間提供額外隔離。
- 容錯與復原有助於提升資訊韌性。
- Mail 與 Messenger 等企業服務運作於更廣泛的安全架構之中。
- 管理活動紀錄可支援稽核與監督。

摘要

Cyberhood 企業安全架構以多層式防護模型為基礎。

此架構結合安全通訊、透過 Independent Firewall 實現的分散式主機防護、身分、授權、資訊保護、惡意程式防護、分散式加密儲存、容錯與復原。

Cyberhood 並非依賴單一安全邊界，而是將防護分布於基礎架構、平台、資訊與應用層。

Cyberhood SPAN 進一步將加密分散式儲存與容錯、復原、惡意程式掃描及多重存取控制屏障結合，以強化此模型。

其結果是一套不僅保護網路周界，更以保護整體企業資訊環境為目標的安全架構。

PART III — 企業平台

企業協作平台

執行概述

Cyberhood 提供企業協作能力，連結組織帳號、即時通訊、郵件、行事曆、工作管理、公告、檔案空間、分享、版本控制、搜尋及跨平台檔案存取。

協作是 Cyberhood 分散式企業平台的原生能力；通訊、資訊管理、工作空間組織、分享與保護，皆以彼此連結的平台能力運作。

6.1 協作作為原生平台能力

Cyberhood 透過組織身分、授權、工作空間、資訊服務與受保護儲存，將協作與資訊管理整合。因此，協作是平台架構的一部分，而不是一組彼此獨立的通訊工具。

協作架構可摘要為：

- 身分 + 通訊 + 工作空間 + 分享 + 資訊管理 + 協作

6.2 組織身分

身分是企業協作的基礎。使用者透過組織帳號參與平台，而權限與角色則決定其與企業資源之間的關係。

此以身分為核心的模型，為通訊、檔案、工作空間與企業應用中的協作提供一致基礎。

6.3 企業通訊

通訊是企業協作的基本組成。Cyberhood 透過 Mail 與 Messenger 提供通訊能力，使組織可在企業平台內維持通訊。

6.4 企業即時通訊

Cyberhood Messenger 提供一對一與群組通訊，並支援文字、圖片、影片及檔案交換。此通訊模型同時支援個人之間的直接通訊與群組成員間的溝通。

6.5 企業郵件

Cyberhood Mail 在平台內提供企業電子郵件能力。電子郵件與組織帳號相關聯，並在企業資訊環境中運作。

6.6 企業工作空間模型

Cyberhood 將協作整合至四種資訊空間：我的空間（My Space）、公共空間（Public Space）、我分享的空間（Sharing With Space）與分享給我的空間（Shared From Space）。這些空間依資訊所有權與分享關係加以區分。

此模型建立清楚的資訊分享方向，區分個人管理資訊、供較廣泛組織成員存取的資訊、使用者分享給他人的資訊，以及他人分享給使用者的資訊。

6.7 我的空間（My Space）

我的空間提供與使用者個人工作空間相關的個人資訊環境，作為該使用者在整體授權架構下管理資訊的位置。

6.8 公共空間（Public Space）

公共空間提供較廣泛組織成員存取的資訊環境，用以區分組織可用資訊與個人工作空間內維護的資訊。

6.9 我分享的空間（Sharing With Space）

我分享的空間代表使用者分享給其他使用者或組織參與者的資訊，清楚呈現資訊由使用者工作空間向外分享的關係。

我分享的空間 → 我分享給其他人的資訊

6.10 分享給我的空間（Shared From Space）

分享給我的空間代表其他使用者或組織參與者分享給該使用者的資訊，清楚呈現透過組織資訊分享關係所接收的資訊。

我分享的空間 → 我分享給其他人的資訊

分享給我的空間 → 其他人分享給我的資訊

此區分使分享資訊的來源與方向更容易理解，並為企業資訊管理建立更清楚的基礎。

6.11 檔案管理與協作

檔案管理是企業協作的基本組成。Cyberhood 將檔案管理與工作空間組織、分享、版本控制、搜尋、授權及受保護儲存連結。

企業資訊生命週期可理解為：建立 → 儲存 → 分享 → 協作 → 版本化 → 搜尋 → 保護。

6.12 版本控制

協作資訊會隨時間持續變化。Cyberhood 將版本控制能力納入資訊管理架構；其協作模型包含 Concurrent Read Concurrent Write（CRCW）與 Concurrent Read Exclusive Write（CREW）模式，以支援版本控制情境。

6.13 全文搜尋

Cyberhood 提供全文搜尋能力以支援資訊探索。目錄、檔案摘要與文件說明可納入全文索引，以支援關鍵字資訊檢索。

6.14 跨平台存取

Cyberhood 平台支援 Windows、Linux、macOS、iPhone、Android 及網頁瀏覽器環境的桌面與行動存取模式。

6.15 同一環境中的通訊與資訊

Cyberhood 將通訊與資訊連結於同一企業環境。使用者可透過 Mail 與 Messenger 溝通，同時在平台中處理檔案、工作空間、分享資訊及組織資源。

6.16 協作與企業工作管理

Cyberhood 的協作環境包含行事曆、工作與公告欄功能，以支援組織通訊及日常協調。

6.17 協作與安全

Cyberhood 將協作與身分、授權、受保護儲存，以及第 5 章所述的多層式安全架構連結。

身分 → 授權 → 協作 → 資訊保護

6.18 協作與 SPAN

Cyberhood SPAN 在協作環境之下提供 Protected Information Layer。因此，檔案管理與協作會與受保護分散式儲存形成架構關係。

6.19 分散式平台上的協作

Cyberhood 的協作環境運作於分散式平台基礎之上。此架構連結分散式基礎架構、分散式平台服務、協作與資訊服務、企業應用及商業服務。

6.20 企業協作模型

完整的 Cyberhood 協作模型，將企業使用者與組織身分連結至 Mail、Messenger、工作空間、資訊服務、分享、版本控制、搜尋與受保護儲存。

關鍵架構原則

- 協作作為原生能力 — 協作整合於 Cyberhood 平台之中。
- 以身分為核心的協作 — 使用者透過組織身分與權限參與。
- 以工作空間為基礎的資訊管理 — 不同工作空間模型支援不同的資訊所有權與協作需求。
- 具方向性的資訊分享 — 我分享的空間與分享給我的空間，區分向外分享的資訊與從他人接收的資訊。
- 整合式通訊 — Mail 與 Messenger 在企業環境內提供通訊能力。
- 資訊連續性 — 檔案、分享、版本控制與搜尋形成連續的資訊生命週期。
- 跨平台可存取性 — Cyberhood 平台支援桌面、行動與瀏覽器環境。
- 受保護的協作 — 協作與身分、授權及受保護資訊連結。
- 分散式協作 — 協作運作於更廣泛的分散式平台基礎之上。

重點摘要

- Cyberhood 提供整合式企業協作環境。
- 協作連結身分、通訊、資訊、工作空間、分享與保護。
- Mail 與 Messenger 提供核心企業通訊能力。
- 我的空間、公共空間、我分享的空間與分享給我的空間，提供不同的資訊分享模型。
- 我分享的空間用以識別使用者分享給其他人的資訊。
- 分享給我的空間用以識別其他人分享給使用者的資訊。
- 版本控制支援資訊可追溯性。
- 全文搜尋支援資訊探索。
- 行事曆、工作與公告欄功能支援組織協調。
- 跨平台存取支援桌面、行動與瀏覽器環境。
- SPAN 在協作環境之下提供受保護儲存層。

摘要

Cyberhood 企業協作平台將通訊、資訊管理、工作空間、分享、版本控制、搜尋及跨平台存取整合於共同的分散式企業環境。

第 7 章

企業應用生態系統與整合

執行概述

Cyberhood 提供整合式企業應用環境，使專業化企業應用在共享的分散式平台架構上運作。企業資訊入口（EIP）、工作流程／電子簽核、ERP、CRM、專案管理、通訊與協作及其他企業應用，各自保留其專業化業務責任，同時參與協調式企業環境。

Cyberhood 企業應用整合是一項已實作的平台能力。API Integration、Transaction Orchestration、Enterprise Service Bus（ESB）、Message Bus、Automatic Cross-Application Synchronization，以及共享的工作流程／電子簽核機制，連接參與應用之間的功能、交易、訊息、資訊流與企業流程。

此架構同時在平台層與企業流程層整合專業化能力。應用可交換資訊、協調交易、參與跨應用工作流程、同步相關應用狀態，並使用共同平台服務，而不需要將各自的專業化業務責任合併成單一巨型應用。

因此，專業化與整合可以共存：企業應用維持專業分工、企業流程受到協調、資訊保持同步，而平台服務維持共享。

7.1 從應用組合走向整合式企業架構

Cyberhood 將分散式企業平台從基礎架構與共享平台服務延伸至整合式企業應用環境。EIP、工作流程／電子簽核、ERP、CRM、專案管理、通訊與協作及其他企業應用，以專業化業務能力運作，同時參與共同的分散式企業架構。

架構目標不是將專業化企業應用合併為單一巨型系統，而是透過已實作的企業整合能力，連接其 API、交易、訊息、資訊流與企業流程，使每個應用保留自身業務責任，同時參與協調式企業營運。

Cyberhood 因此將企業應用整合視為平台能力，而不是彼此孤立的點對點連線集合。

企業應用整合不要求功能趨同。

企業應用維持專業化；企業流程受到協調；資訊保持同步；平台服務維持共享。

7.2 企業應用整合架構

Cyberhood 企業應用整合架構由一組彼此關聯的架構責任構成。企業應用提供專業化業務功能；共享工作流程與企業流程機制跨越應用邊界協調組織程序；企業整合服務提供 API 交換、交易編排、服務與訊息通訊，以及跨應用自動同步等已實作機制；Cyberhood Platform Core Services 提供共同的身分、授權、資訊、協作、通訊、管理與安全關係；Cyberhood SPAN 為適用資訊提供受保護資訊層；分散式基礎架構則提供底層運算、儲存、網路、站點、邊緣、資料中心與雲端資源。

企業使用者與組織環境 → 專業化企業應用 <-> 共享企業流程與工作流程整合 <-> 企業整合服務 <-> Cyberhood Platform Core Services <-> Cyberhood SPAN <-> 分散式基礎架構

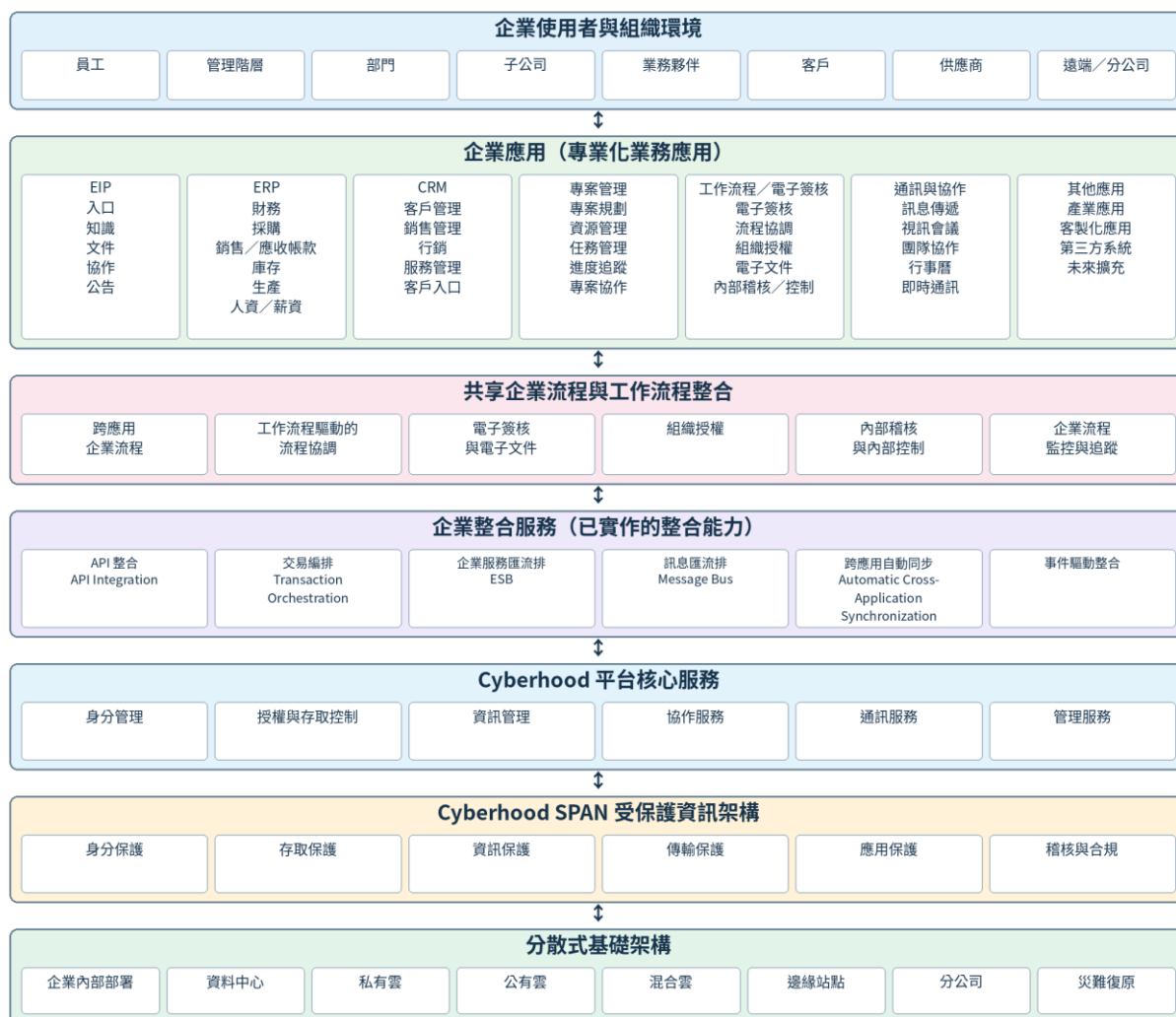


圖 7-1 Cyberhood 企業應用整合架構

透過共享工作流程、企業整合服務、共同平台服務、Cyberhood SPAN 與分散式基礎架構整合專業化企業應用

圖 7-1 — Cyberhood 企業應用整合架構

圖 7-1 所呈現的關係對應 Cyberhood 已實作的功能能力。專業化企業應用透過 API Integration、Transaction Orchestration、ESB、Message Bus、Automatic Cross-Application Synchronization、共同平台服務、受保護資訊架構與分散式基礎架構，參與共享工作流程與企業流程。

7.3 專業化企業應用

Cyberhood 在應用層保留專業化，因為不同企業責任需要不同的業務邏輯、資訊模型與營運流程。整合的目的在於連接責任，而不是消除責任邊界。

企業資訊入口（EIP）— 提供組織資訊與工作環境，讓使用者存取企業資訊、服務與應用能力。

工作流程／電子簽核 — 支援結構化組織流程，同時作為跨應用流程協調能力。

ERP — 支援銷售與應收帳款、採購與應付帳款、會計、資產與資金、庫存與成本分析、生產與排程、人力資源與薪資、預算，以及外包工程／勞務支出管理。

CRM — 支援客戶互動、客戶資訊、服務歷程、問題、產品回饋及相關客戶活動。

專案管理 — 支援專案規劃、執行、協調、進度管理、專案資訊與協作。

通訊與協作 — 透過企業通訊與協作工作能力連接人員、資訊與業務活動。

其他企業應用 — 可透過 Cyberhood 提供的整合機制參與整合式環境。

業務責任各自專業化；平台服務共享。

7.4 已實作的企業整合服務

Cyberhood 提供已實作的企業整合服務，在功能、交易、訊息、資訊與企業流程層級連接專業化應用。這些能力是實際企業應用環境的一部分，而不只是概念性的整合模型。

7.4.1 API Integration

API Integration 透過已定義的應用介面，使參與的應用與服務交換功能能力與資訊，在不將專業功能合併至同一應用的前提下提供整合路徑。

7.4.2 交易編排（Transaction Orchestration）

Transaction Orchestration 協調跨越應用邊界的業務活動。源自一個應用的交易可參與涉及其他應用的工作流程、授權、控制、處理與同步序列。

7.4.3 Enterprise Service Bus（ESB）

Cyberhood ESB 提供共享的企業整合機制，使服務與應用參與協調式互動，降低對孤立應用對應用關係的依賴，並支援共同整合架構。

7.4.4 Message Bus

Message Bus 支援參與應用與平台元件之間的訊息式通訊，使訊息與流程事件可參與跨應用處理，而不要求所有功能在單一應用中執行。

7.4.5 Automatic Cross-Application Synchronization

Automatic Cross-Application Synchronization 維持參與應用之間相關資訊與流程狀態的關係。當整合式企業流程改變資訊或到達定義的流程狀態時，可在整合環境中同步對應的應用關係。

API Integration → Transaction Orchestration → 訊息與服務交換 → 流程協調 → Automatic Cross-Application Synchronization

7.5 工作流程作為跨應用流程協調機制

工作流程／電子簽核既是專業化企業應用能力，也是 Cyberhood 企業應用環境中的跨應用流程協調機制。

來自 ERP、CRM、專案管理、EIP 或其他整合應用的業務事件與交易，可啟動、參與或回應工作流程驅動的程序。工作流程提供共享流程關係，使應用所產生的活動能經過電子簽核、電子文件、組織授權、內部稽核、內部控制與後續業務處理。

透過 API Integration、Transaction Orchestration、ESB、Message Bus 與 Automatic Cross-Application Synchronization，工作流程狀態與結果可參與相關應用後續處理。

工作流程不只是核准交易 — 它連接跨企業應用的業務流程。

7.6 電子簽核、內部稽核與內部控制

電子簽核為整合式企業流程提供結構化的組織決策機制。它不只是獨立的簽核應用，而可參與由企業應用啟動的流程，並將核准、駁回或完成等流程狀態交付後續業務處理。

內部稽核與內部控制透過工作流程／電子簽核引擎連接企業營運，使稽核與控制要求可與業務交易、組織授權、佐證文件、流程紀錄及後續應用處理建立關聯。

業務活動 → 工作流程／電子簽核 → 組織授權 → 內部控制／內部稽核 → 後續業務處理 → 跨應用同步

例如，採購活動可源自 ERP，進入電子簽核流程，經過必要的組織授權與控制程序，保留相關流程紀錄與佐證文件，再繼續進入 ERP 或相關應用的後續處理。工作流程負責協調流程，而不取代 ERP 的專業化責任。

7.7 跨應用企業流程範例

同一套架構可支援跨越不同專業化應用的企業流程。以下關係用以說明架構模式，而不重新定義參與應用的責任。

ERP 交易 → 工作流程／電子簽核 → 授權與控制 → 後續 ERP 處理 → 與參與應用同步。

CRM 活動 → 工作流程或相關組織流程 → 授權／協作 → 後續客戶或企業處理。

專案活動 → 工作流程／電子簽核 → 組織授權 → 專案處理與相關資訊同步。

EIP 使用者活動 → 應用或工作流程服務 → 企業處理 → 資訊與狀態回到整合式工作環境。

應用擁有專業化業務責任；整合架構連接企業流程。

7.8 企業資訊入口（EIP）

EIP 提供組織資訊與工作環境，使企業使用者可存取資訊、應用、協作能力與企業流程。在整合架構中，EIP 可作為面向企業使用者的入口環境，而底層應用責任仍分布於專業化應用與共享平台服務。

此關係使使用者體驗可以在組織層面統一，而不要求底層企業應用在功能上變得相同。

7.9 客戶關係管理（CRM）

CRM 保留客戶導向活動與資訊的責任。當需要組織工作流程、企業資訊、協作或後續業務處理時，客戶互動、服務歷程、問題、產品回饋與相關客戶流程可參與更廣泛的整合架構。

CRM 整合因此在保留 CRM 專業化業務能力的同時，連接客戶責任與企業流程。

7.10 企業資源規劃（ERP）

ERP 保留企業資源與營運流程的責任。Cyberhood ERP 環境包括銷售與應收帳款、採購與應付帳款、會計、資產與資金、庫存與成本分析、生產與排程、人力資源與薪資、預算，以及外包工程／勞務支出管理。

在整合架構中，ERP 交易可參與工作流程、電子簽核、交易編排、訊息交換與跨應用同步，使營運交易成為組織流程的一部分，而不將底層 ERP 責任移轉至工作流程或整合層。

ERP 擁有營運交易；工作流程協調組織程序；整合服務連接參與系統。

7.11 專案管理

專案管理保留專案導向規劃與執行責任。當專案工作需要組織授權或與其他企業應用互動時，專案活動可參與共享工作流程、簽核、協作、資訊管理與整合服務。

因此可連接專案流程與企業營運，而不要求專案管理重複 ERP、CRM 或工作流程的責任。

7.12 整合流程中的通訊與協作

整合式企業流程同時涉及人員與系統。Cyberhood 通訊與協作能力提供人員互動環境，使使用者能溝通、交換資訊並參與業務活動。

協作可與工作流程及企業應用共同運作，使組織通訊與業務處理保持連結，而不是形成彼此分離的資訊孤島。

7.13 共同平台服務

企業整合運作於共同的 Cyberhood Platform Core Services 之上。身分與授權決定誰可參與應用與流程；資訊服務管理企業資訊關係；通訊與協作服務連接使用者與活動；管理與安全服務提供共同的平台層控制。

共享平台服務可降低每個企業應用各自建立獨立架構基礎的需求。

專業化應用 → 共享企業流程 → 企業整合服務 → 共同平台服務 → 分散式基礎架構

7.14 企業應用整合與 Cyberhood SPAN

企業應用整合與受保護資訊架構彼此相關但在架構上不同。整合決定應用、交易、訊息與企業流程如何互動；Cyberhood SPAN 決定套用 SPAN 保護的資訊如何分段、加密、分散配置、重建並恢復至所需保護狀態。

因此 SPAN 不取代企業應用整合，企業應用整合也不取代資訊保護。當應用資訊採用 SPAN 保護時，兩者共同參與更廣泛的 Cyberhood 平台架構。

應用整合 ≠ 資訊保護 — 兩者共同參與同一企業架構。

7.15 企業應用整合與分散式基礎架構

整合式企業應用不要求所有應用功能、資訊或基礎架構資源位於同一實體位置。Cyberhood 分散式平台架構允許企業應用環境依部署模式跨參與的基礎架構運作。

因此，應用之間的邏輯整合關係與支援它們的應用及基礎架構資源之實體配置是不同的架構責任。

應用整合定義業務與服務關係；部署定義參與資源在何處運作。

7.16 企業應用整合與安全

跨應用整合仍受 Cyberhood 安全架構約束。當企業流程跨越應用邊界時，身分、驗證、授權、安全通訊、平台安全控制與受保護資源關係仍持續適用。

身分 → 驗證 → 授權 → 整合式企業流程 → 受保護資源

7.17 整合式應用環境的架構價值

Cyberhood 企業應用整合的架構價值，在於無須要求功能趨同即可連接專業化應用。應用可依自身業務責任演進，同時持續參與共同的流程、整合、平台、資訊與基礎架構關係。

已實作的 API Integration、Transaction Orchestration、ESB、Message Bus 與 Automatic Cross-Application Synchronization，使應用專業化與企業協調得以共存。

整合不要求一致化。

專業化應用可以演進，而共享平台架構維持一致。

7.18 企業應用整合模型

Cyberhood 企業應用環境可概括為從專業化業務能力走向協調式企業營運的演進：

專業化應用 → API 與訊息整合 → Transaction Orchestration → 工作流程與流程整合 → 資訊同步 → 組織協調 → 企業營運

此模型連接企業應用、組織流程、企業資訊、平台服務與分散式基礎架構，同時維持清楚的架構責任。

7.19 關鍵架構原則

企業應用整合是 Cyberhood 已實作的平台能力。

企業應用依其業務責任維持專業化。

工作流程／電子簽核提供跨應用流程協調。

內部稽核與內部控制透過工作流程／電子簽核引擎參與企業流程。

API Integration 連接應用功能與資訊。

Transaction Orchestration 協調跨應用邊界的業務活動。

ESB 與 Message Bus 提供共享的服務與訊息整合機制。

Automatic Cross-Application Synchronization 維持相關資訊與流程狀態關係。

共同平台服務提供共享架構基礎。

Cyberhood SPAN 在套用 SPAN 保護時提供受保護資訊架構。

分散式基礎架構提供整合環境運作所需的實體資源。

7.20 結論

Cyberhood 企業應用整合將專業化企業應用組合轉化為協調式企業應用環境。ERP、CRM、EIP、專案管理、工作流程／電子簽核、通訊與協作及其他應用保留專業化責任，同時參與共享企業流程與共同平台關係。

已實作的整合架構透過 API Integration、Transaction Orchestration、ESB、Message Bus 與 Automatic Cross-Application Synchronization，連接 API、交易、訊息、資訊流、工作流程狀態與應用資料關係。

此架構使 Cyberhood 能在不強迫應用進入單一巨型功能模型的情況下連接企業應用。專業化應用維持專業化；平台提供共同運作所需的機制。

專業化應用 — 整合式流程 — 共享平台服務 — 一個企業架構。

Cyberhood 不只是將企業應用放在共同平台上，而是在共享企業架構中整合其 API、交易、訊息、資訊流與企業流程。

第 8 章

開發者平台與分散式應用框架

執行概述

Cyberhood 分散式企業平台不僅提供基礎架構、協作服務與企業應用，也旨在建立分散式企業應用的共同開發基礎。

Cyberhood SDK 提供分散式系統應用程式設計框架，使應用可與平台的分散式服務及企業資源形成架構關係。在此架構中，應用開發與底層分散式基礎架構的複雜性分離。用戶端應用可專注於呈現與使用者互動，而伺服器端服務則在分散式平台環境中執行應用邏輯與處理。

因此，開發者架構可概括為：應用程式 → Cyberhood SDK → 分散式平台服務 → 分散式基礎架構。

此模型使 Cyberhood 從一組企業能力，進一步延伸為可擴充的分散式應用平台。

8.1 Developer Platform 作為架構層

企業平台必須隨組織需求變化而持續演進。

標準化企業應用可處理常見營運需求，但組織也可能需要專用應用、新的業務流程，或針對特定產業與營運環境設計的應用服務。

Cyberhood 透過建立在同一分散式架構上的 Developer Platform 回應此需求，而該架構亦支撐整體 Cyberhood 環境。

Developer Platform 建立以下關係：開發者 → 應用程式 → 平台服務 → 分散式資源。

Cyberhood 不將應用開發視為獨立的技術環境，而是將其置於分散式平台架構之中。

因此，新應用可透過明確的架構路徑，與既有企業服務共同運作。

8.2 Cyberhood SDK

Cyberhood SDK 提供分散式平台的應用開發介面。其目的在於提供開發者一套共同框架，用以依據 Cyberhood 的分散式資料處理架構開發應用。

在概念上，SDK 在應用開發與底層分散式環境之間建立抽象層：

應用程式 → Cyberhood SDK → 分散式平台服務 → 分散式基礎架構

因此，應用是透過平台架構與分散式環境互動，而不是只以單一獨立伺服器為設計中心。

此一區別是 Cyberhood 開發者模型的核心。

8.3 分散式應用框架（Distributed Application Framework）

傳統企業應用經常圍繞預先指定的伺服器或固定的基礎架構關係設計。

Cyberhood 導入分散式應用模型，使應用執行與分散式平台資源形成關係。

此框架可由四個架構元素理解：身分 + 服務選擇 + 應用處理 + 分散式資源。

這些元素建立一套開發模型，使應用可參與 Cyberhood 分散式環境。

由此形成的架構，將應用體驗與個別基礎架構資源的實體位置分離。

8.4 分散式身分驗證

身分是 Cyberhood 的基礎平台能力。

如前述章節所建立，組織帳號是驗證、授權、協作及存取企業資訊的基礎。Developer Platform 將此身分關係延伸至分散式應用執行。

概念上的應用存取順序可表示為：使用者 → 身分驗證 → 應用服務 → 企業資源。

在存取應用服務與受保護資源之前，身分驗證先建立使用者與分散式平台之間的關係。

因此，應用執行可運作於 Cyberhood 全平台共同使用的身分架構之中。

8.5 分散式服務選擇

Cyberhood 分散式應用模型的重要特性之一，是可依平台架構選擇適當的分散式服務資源。

分散式身分驗證流程可依平台模型辨識適當的分散式主機，包括較接近或效能較佳的主機，以支援應用執行。

概念上可表示為：使用者／用戶端 → 身分驗證 → 分散式服務選擇 → 分散式主機 → 應用服務。

此架構降低應用與單一預先指定應用主機之間的概念性依賴。

服務選擇機制成為分散式平台關係的一部分，而不是特定應用對基礎架構的假設。

8.6 用戶端與伺服器端的應用責任

Cyberhood 應用模型區分伺服器端應用處理，以及用戶端的呈現與互動。此分離建立兩項主要應用責任。

用戶端責任主要著重於使用者呈現、使用者互動、應用介面行為，以及與應用服務的通訊。

伺服器端責任主要著重於應用邏輯、應用處理、與平台服務互動，以及應用相關資訊的處理。

其關係可表示為：用戶端呈現與互動 ↔ 伺服器端應用邏輯與處理。

此分離為分散式應用開發提供清楚的架構模型。

8.7 分散式應用處理

在 Cyberhood 架構中，應用處理並非獨立於分散式平台之外。伺服器端應用處理與分散式平台服務及基礎架構資源形成關係。

概念上可表示為：用戶端 → 應用介面 → 分散式應用服務 → 應用處理 → 平台資源。

因此，分散式平台提供應用服務運作所需的執行基礎。

這使 Developer Framework 能與更廣泛的 Cyberhood 分散式架構保持一致。

8.8 共用平台服務

在 Cyberhood 環境中運作的應用，可在架構上與共用平台服務連結。Cyberhood 架構框架（Cyberhood Architecture Framework, CAF）定義的分散式平台能力包括身分驗證、授權、索引、分散式儲存服務、工作流程、訊息傳遞、SDK 服務及管理。這些共用能力在應用與基礎架構之間形成架構服務層。

此模型的重要意義在於架構一致性。

新應用可依循支援既有 Cyberhood 服務的同一平台基礎進行設計。

8.9 資訊與儲存服務

企業應用會產生、處理並使用資訊。

因此，Cyberhood 將應用開發置於更廣泛的平台資訊架構中，而不是將應用資訊視為完全獨立的架構領域。應用可與平台資訊及分散式儲存服務形成關係。

由此建立概念關係：應用程式 → 資訊服務 → 分散式儲存架構。

第 4 章所述的 Cyberhood SPAN 提供平台的受保護分散式資訊儲存層。然而，此架構並不假設每一個應用或每一類應用資料都必須自動透過 SPAN 儲存。

應用與受保護儲存之間的具體關係，取決於應用設計及其對平台服務的使用方式。此區別維持 Developer Framework 與個別應用所採用儲存實作之間的分離。

8.10 應用的安全與授權

應用擴充能力必須持續與企業安全相連。

因此，Cyberhood 將應用存取置於第 5 章所建立的身分與授權架構之中。

概念關係為：身分 → 驗證 → 授權 → 應用程式 → 受保護資源。

驗證確認使用者是誰。

授權決定在何種條件下可以存取資源。

應用程式提供使用者與這些資源互動所需的業務或營運能力。

此架構使應用開發與更廣泛的 Cyberhood 企業安全模型保持一致。

8.11 應用與協作服務整合

第 6 章已將協作建立為 Cyberhood 分散式企業平台的原生能力。Developer Platform 進一步延伸此架構關係，提供應用與協作及資訊服務共存的基礎。

此架構使協作、資訊管理與應用服務可存在於共同的分散式環境中。它也為業務流程涉及組織使用者、共享資訊、通訊或協作活動的應用提供基礎。

8.12 應用與企業服務整合

第 7 章說明 Cyberhood 企業應用生態系統與整合，包括工作流程、專案管理、CRM 與 ERP。

第 8 章則透過提供額外應用與企業能力的開發框架，延伸此架構模型。

因此，其關係可表示為：既有企業應用 + 可擴充應用 → 共用分散式平台。

這並不表示每個應用都必須執行相同功能或採用相同實作。相反地，它建立共同架構基礎，使不同企業應用可參與更廣泛的 Cyberhood 環境。

第 7 章定義企業應用能力；第 8 章定義應用開發與擴充的架構基礎。

8.13 分散式應用執行模型

Cyberhood 開發者架構可透過分散式應用執行模型加以概括。

此模型呈現數項架構原則。

第一，應用不被視為孤立的軟體元件。

第二，身分提供使用者進入分散式環境的起始關係。

第三，分散式服務選擇將應用執行與適當的平台資源連結。

第四，應用處理可與共享平台及資訊服務形成關係。

最終的執行模型可概括為：驗證 → 選擇服務 → 執行應用 → 存取平台資源。

8.14 應用擴充性

擴充性是 Cyberhood 開發者平台（Developer Platform）的核心目的。

Cyberhood SDK 與共用平台架構為新應用整合既有分散式服務與企業資源提供路徑。

這表示此架構不受限於固定的一組應用。隨著組織需求演進，可在分散式平台基礎上開發額外的應用能力。

因此，既有應用與新開發應用都可定位於同一個更廣泛的平台架構中。

這為應用的長期演進建立基礎，而不需要每次導入新業務功能時，就在概念上取代底層分散式架構。

8.15 Cyberhood 作為企業應用平台

開發框架（Developer Framework）改變了 Cyberhood 的架構角色。若沒有應用開發框架，Cyberhood 主要可能被視為分散式基礎架構與預先定義企業應用集合的組合。

Cyberhood SDK 引入另一個架構面向：Cyberhood 成為可開發與擴充分散式企業應用的平台。

因此，架構演進可表示為：分散式基礎架構 → 分散式平台服務 → Developer Framework → 企業應用 → 業務服務。

此演進將基礎架構工程與應用開發及組織業務能力連結。它也在第 7 章所述的企業應用生態系統與整合架構，以及第 9 章的部署架構之間建立架構橋接。

8.16 Developer Platform 架構模型

完整的 Cyberhood Developer Platform 建立應用、SDK、共用平台服務與分散式基礎架構之間的關係。

此模型可概括為：企業應用 → Cyberhood SDK → Distributed Application Framework → 身分／授權／資訊服務 → 分散式平台 → 分散式基礎架構。

它也呈現 Developer Framework 在更廣泛的 Cyberhood 架構框架（CAF）中的角色。

基礎架構提供資源；平台服務提供共用能力；SDK 提供應用開發基礎；應用則將平台能力轉化為企業服務。

關鍵架構原則

- 分散式應用基礎 — Cyberhood 提供以平台分散式系統架構為核心設計的 SDK 與應用框架。
- 應用責任分離 — 用戶端呈現與互動，與伺服器端應用邏輯及處理分離。
- 身分作為應用進入點 — 分散式應用執行與 Cyberhood 身分驗證形成關係。
- 分散式服務選擇 — 平台模型可將應用執行與適當的分散式主機建立關聯，而非假設單一預先指定伺服器。
- 共享平台服務 — 應用可與共用的身分、授權、資訊、工作流程、訊息傳遞、儲存及管理服務形成關係。
- 安全延續性 — 應用存取持續與企業平台的身份及授權架構相連。
- 應用擴充性 — SDK 提供新應用整合分散式服務與企業資源的架構路徑。
- 平台層級開發 — 應用開發成為 Cyberhood 平台架構的一部分，而非與基礎架構及企業服務脫節的獨立層。

重點摘要

- Cyberhood SDK 為分散式應用提供共同的開發基礎。
- Developer Framework 運作於 Cyberhood 分散式基礎架構與平台服務層之上。
- 分散式身分驗證建立使用者與應用服務之間的關係。
- 分散式服務選擇可將應用執行與適當的平台主機建立關聯。
- 用戶端呈現與互動，與伺服器端應用邏輯及處理分離。
- 應用可與共用平台及資訊服務形成關係。
- 身分與授權將應用存取與企業安全連結。
- 開發框架使 Cyberhood 超越預先定義的應用環境。
- 既有 Cyberhood 應用與新開發應用，可共同參與同一個更廣泛的分散式平台架構。
- SDK 在分散式基礎架構與可擴充企業應用之間建立架構橋接。

摘要

Cyberhood Developer Platform 與 Distributed Application Framework 將 Cyberhood 架構從基礎架構、協作及預先定義的企業應用，延伸至可擴充的應用開發環境。

此架構的核心是 Cyberhood SDK，它依據平台的分散式資料處理架構提供共同的開發基礎。

此框架將用戶端呈現與互動，與伺服器端應用邏輯及處理分離；同時，分散式身分驗證與服務選擇將應用執行連結至更廣泛的分散式平台。

應用可與身分、授權、資訊服務、工作流程、訊息傳遞、分散式資源及受保護資訊架構等共用能力形成關係。

最終的開發模型可概括為：使用者 → 驗證 → 分散式服務選擇 → 應用程式 → 平台服務 → 分散式資源。

透過此架構，Cyberhood 建立以下演進關係：分散式基礎架構 → 平台服務 → Developer Framework → 企業應用 → 業務服務。

因此，Developer Framework 為 Cyberhood 隨組織需求演進而持續擴充提供架構基礎，同時維持與整個平台既有的分散式基礎架構、安全、協作及企業應用模型之間的連續性。

Developer Platform 與企業整合服務

Cyberhood SDK 與 Distributed Application Framework 與第 7 章所建立的 Enterprise Integration Services 協同運作。為 Cyberhood 環境開發的應用可參與更廣泛的平台架構，同時依其業務責任維持專業化。

已實作的 API Integration、Transaction Orchestration、ESB、Message Bus 與 Automatic Cross-Application Synchronization，提供參與應用交換資訊、協調交易、傳遞訊息與參與跨應用流程的整合機制。

SDK 與應用框架提供開發基礎；Enterprise Integration Services 提供跨應用整合能力；Platform Core Services 提供共同企業服務；Distributed Infrastructure 提供參與的執行資源。

Cyberhood 不要求每個應用使用所有整合機制，也不要求所有應用資訊都採用 SPAN 保護。整合與保護依應用及部署需求套用。

應用 → Cyberhood SDK / Distributed Application Framework → Integration Interfaces → Enterprise Integration Services → Cyberhood Platform Services → Distributed Infrastructure

應用開發與應用整合彼此相關，但在架構上不同。

PART IV — 架構

部署模式與參考架構

執行概述

Cyberhood 分散式企業平台可運作於多樣化的企業基礎架構環境。

企業可能在單一據點、多個辦公室與營運站點、企業自主管理的基礎架構、私有雲，或私有與外部基礎架構混合的環境中運作。

Cyberhood 提供可依這些需求調整的分散式平台架構，而不必因每一種實體拓撲重新定義企業平台。

Cyberhood 將邏輯企業平台架構與其所運作的實體基礎架構拓撲分離。企業應用、協作服務、身分與授權、受保護資訊、分散式處理及平台服務維持於共同架構中；底層運算、儲存、網路、節點與站點資源則可依組織需求演進。

一套平台架構 — 多種部署模式。

部署關係可表示為：企業需求 → 部署模式 → Cyberhood 平台架構 → 分散式基礎架構資源。

本章涵蓋私有企業、私有雲、混合雲、多站點企業、分散式本地節點（Distributed Local Node, DLN）及復原導向部署。這些特性不必互斥，可依基礎架構策略、地理分布、營運需求、資訊保護需求及服務持續性目標組合使用。

部署決定平台資源在哪裡運作；

平台架構決定企業能力如何與這些資源形成關係。

9.1 部署架構原則

分散式企業平台必須支援不同基礎架構環境，而不需要為每一種部署情境重新設計企業架構。Cyberhood 透過分離邏輯平台能力與其底層實體基礎架構來達成此目標。

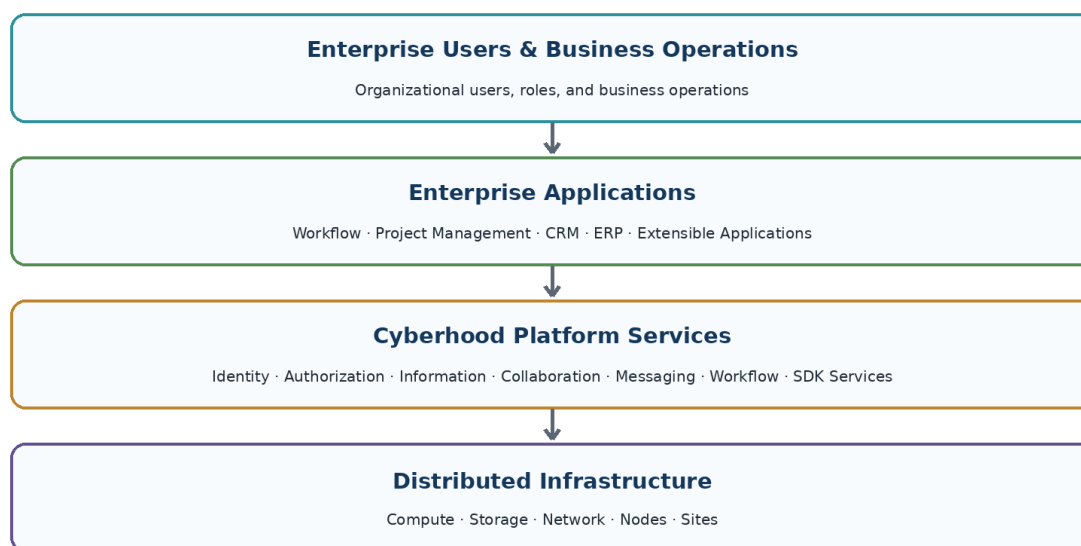


圖 9-1 — Cyberhood 四層部署架構

分散式基礎架構提供支援平台所需的實體和虛擬資源。Cyberhood 平台服務在這些資源之上提供通用功能。企業應用程式利用平台基礎架構來提供專門的組織功能。企業使用者和業務營運根據組織角色和營運需求與由此產生的應用程式和服務進行互動。

- 基礎架構分佈 — 運算、儲存、網路、節點和站點可以根據部署要求進行分佈。
- 平台一致性 — Cyberhood 平台服務在底層基礎架構拓撲之上提供共同的架構基礎。
- 應用不依賴單一基礎架構位置 — 企業應用透過平台運作，而非僅由某一實體伺服器位置所定義。
- 分散式資訊資源 — 資訊服務可與分散式及受保護的儲存資源形成架構關係。
- 模組化演進 — 部署容量可隨組織需求變化而演進。

邏輯平台架構與實體部署拓撲彼此相關，但在架構上有所區別。

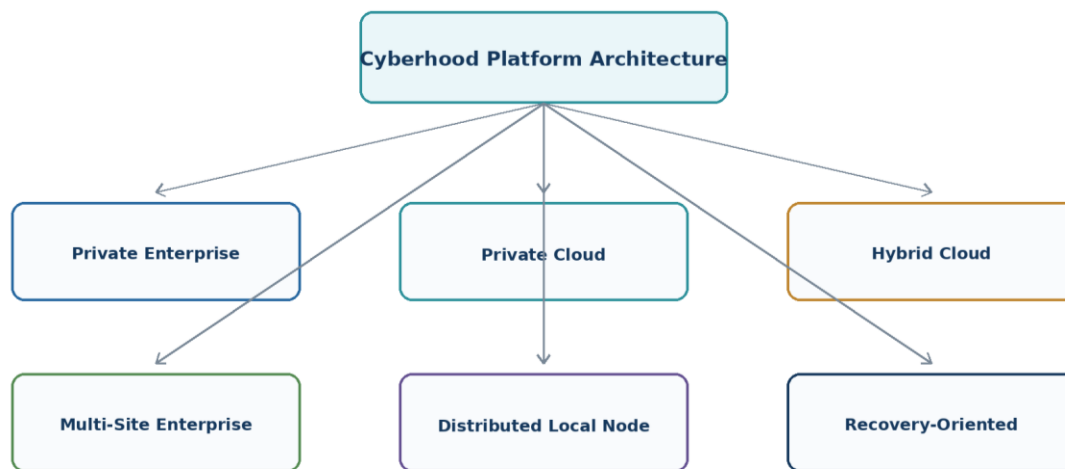


圖 9-2 — Cyberhood 部署模式

9.2 私有企業部署

私有企業部署將 Cyberhood 基礎架構置於組織控制的環境中，可包含企業運算、儲存、內部網路、節點及其他技術資源。

Cyberhood 在此環境中提供身分、授權、協作、資訊服務、企業應用與分散式處理的共同平台基礎。私有部署不要求所有資源位於同一實體地點；企業控制的資源可分布於總部、資料中心、分公司、營運設施或其他組織位置。

私有部署 ≠ 單一站點部署

私有企業部署定義的是控制環境，而不是強制性的實體拓撲。

9.3 私有雲部署

私有雲部署擴展了私有企業模式，它將運算、儲存、網路和平台資源組織在由組織控制或專用於組織的面向雲端的基礎架構環境中。

私有雲提供基礎架構資源；Cyberhood 則提供運作於其上的分散式企業平台。

Cyberhood 的身分、授權、協作、資訊管理、企業應用與分散式處理仍屬平台架構；底層則依組織私有雲策略配置。本概念模型不依賴特定基礎架構供應商、虛擬化平台或雲端實作。

雲端基礎架構 ≠ 企業平台。

9.4 混合雲部署

混合雲部署可結合企業自主管理的基礎架構與外部或雲端資源，同時維持共同的 Cyberhood 平台架構。重點不是單純將應用從一個環境搬到另一個環境，而是讓適當資源依部署需求參與分散式平台。

實際網路、基礎架構整合、安全控制、連線與營運設定取決於組織選擇的環境；因此 Cyberhood 混合架構不依賴特定公有雲供應商。

基礎架構可以不同；平台架構保持一致。

混合部署本身不代表自動工作負載遷移、通用應用可攜性、雲原生編排或自動地理容錯移轉。

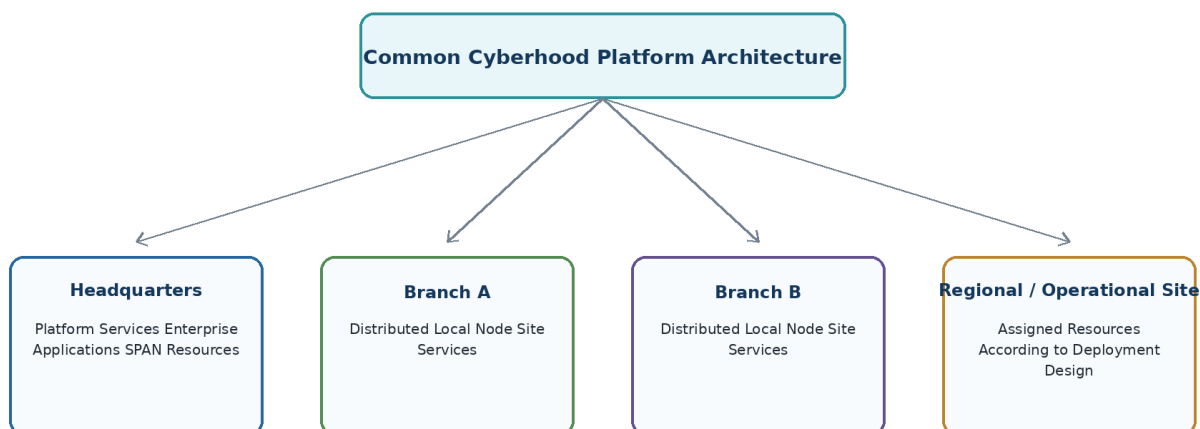
9.5 多站點企業部署

許多企業在多個實體地點運營，包括總部、分支機構、區域設施、營運站點和其他組織環境。Cyberhood 的分散式架構為這些地點融入更廣泛的企業平台架構提供了基礎。

每個地點可以根據其營運角色、可用基礎架構、分配的平台服務和部署要求參與其中。多站點架構並不要求每個地點都擁有相同的基礎架構或執行相同的平台職責。

共同平台架構不要求站點架構完全一致。

多站點描述的是地理拓撲；它本身不代表 Active-Active、每站相同應用部署、全面資訊複寫、自動地理容錯移轉或預先定義的 RPO/RTO。



Central Coordination Does Not Require Complete Centralization

圖 9-3 — 多站點企業與分散式本地節點架構

9.6 分散式本地節點部署

分散式本地節點（Distributed Local Node, DLN）提供將 Cyberhood 平台能力延伸至分散式組織據點的架構機制。DLN 可參與整體 Cyberhood 環境，並與特定站點的使用者、服務、處理需求、儲存架構與基礎資源形成關係。

DLN 的實際角色取決於部署設計及該站點被賦予的責任；不應解讀為每個站點都必須部署完全相同的設備或服務配置。

分散式本地節點（**Distributed Local Node, DLN**）將平台延伸至站點；其所承擔的責任取決於部署設計。

分散式本地節點 ≠ 獨立的本地系統

9.7 總部與分公司架構

常見企業情境包含總部與一個或多個分公司。Cyberhood 可透過分散式架構，使中央與本地資源共同參與同一平台拓撲。

總部可承擔中央平台責任、企業服務或組織資源；分公司則透過適當指派的分散式資源參與。這不表示所有 Cyberhood 服務都必須集中於總部。

集中協調不等於完全中央集中。

架構可依各站點的規模、工作負載、可用基礎架構與營運角色持續演進。

9.8 地理分散架構

Cyberhood 可將分散式基礎架構延伸至地理分離的總部、分公司、區域設施、營運站點、資料中心及其他環境。

地理基礎架構分布

定義運算、儲存、網路、節點及其他資源的實體位置。

地理服務分布

定義平台與應用服務責任在哪裡運作。

地理資訊保護

定義受保護企業資訊如何透過 Cyberhood SPAN，在地理分離的儲存資源之間參與資訊保護。

地理基礎架構分布 ≠ 自動服務分布、

地理服務分布 ≠ 自動地理容錯移轉

地理資訊保護 ≠ 自動 Active-Active 服務架構

地理分散可提供降低對單一實體位置不必要依賴的架構基礎，但實際運作行為仍取決於參與服務與部署設定；它不會自動建立 Active-Active 區域架構、全面複寫或自動地理容錯移轉。

9.9 高可用性部署模型

第 3 章將高可用性（High Availability, HA）定義為包含分散式資源、故障偵測、資源隔離、重新分配、復原及容量恢復的架構能力；本章將其套用於部署拓撲。

HA 部署的目的，是降低對單一基礎架構元件的不必要依賴，並建立服務持續性機制可運作的架構基礎。

僅有多個資源並不構成高可用性。

HA 取決於分散式資源、故障偵測、隔離、服務或工作負載重新分配與復原之間的關係，不代表每個應用、服務或資源都具有相同可用性。

分散式部署建立 HA 基礎；實際可用性取決於部署設定與參與服務。

服務配置

Cyberhood SPAN 在部署架構中提供 Protected Information Layer。企業應用與資訊服務操作邏輯企業資訊；SPAN 則管理該資訊跨參與儲存資源的分散式受保護表示形式。

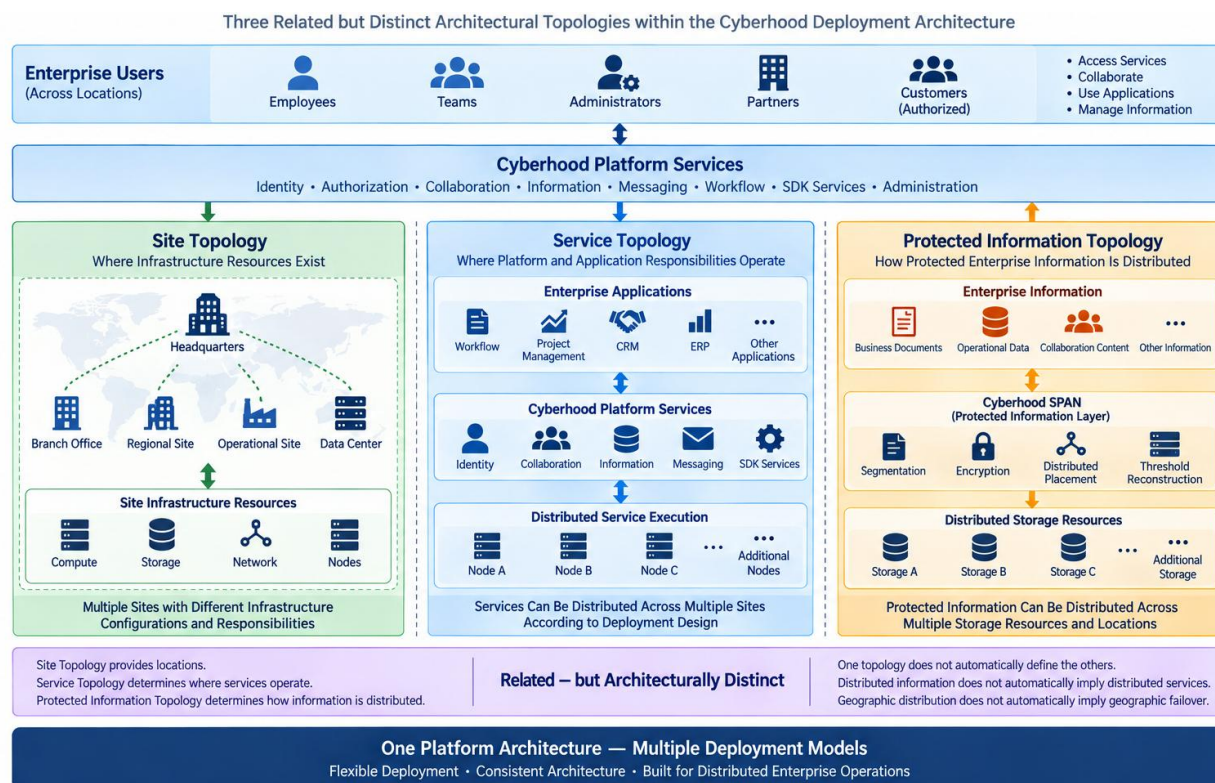


圖 9-4 — 站點、服務與受保護資訊拓撲。服務配置定義平台與應用處理責任在哪裡運作；受保護資訊配置定義 SPAN 資訊如何分散於參與儲存資源

服務配置

定義平台與應用處理責任在哪裡運作。

受保護資訊配置

定義受 SPAN 保護的資訊如何分散於參與的儲存資源。

服務配置與受保護資訊配置彼此相關，但在架構上有所區別。

應用位置 ≠ 完整資訊位置

受保護資訊分布 ≠ 自動應用分布

在保護與部署設計支援的情況下，受保護資訊元件可跨地理分離的基礎架構參與。地理分散的受保護資訊配置不會自動建立地理服務容錯移轉。

9.11 復原導向部署

高可用性與復原導向架構處理相關但不同的營運目標。高可用性主要處理參與資源或服務不可用時的服務持續性；復原導向架構則處理中斷超過現行環境持續能力後的服務恢復。



圖 9-5 — 高可用性與復原導向架構

高可用性 → 持續服務；
復原導向架構 → 恢復服務。

服務持續性與復原之間的界線，取決於部署架構、參與服務、可用資源及中斷性質。復原導向部署可使用分散式基礎架構與地理分離資源，作為組織整體營運持續架構的一部分。

分散式架構提供復原的基礎，但本身不定義復原政策。

Cyberhood 平台架構不預設通用的復原點目標（RPO）、復原時間目標（RTO）或自動災難復原政策；這些要求必須依組織需求與實際部署設定決定。

9.12 跨部署模式的安全架構

部署拓撲可以改變，但 Cyberhood 企業安全架構的基本原則仍適用於私有企業、私有雲、混合雲、多站點、DLN 與復原導向環境。企業資源存取持續與身分、驗證、授權、通訊保護、主機保護、惡意程式防護及受保護資訊相連。

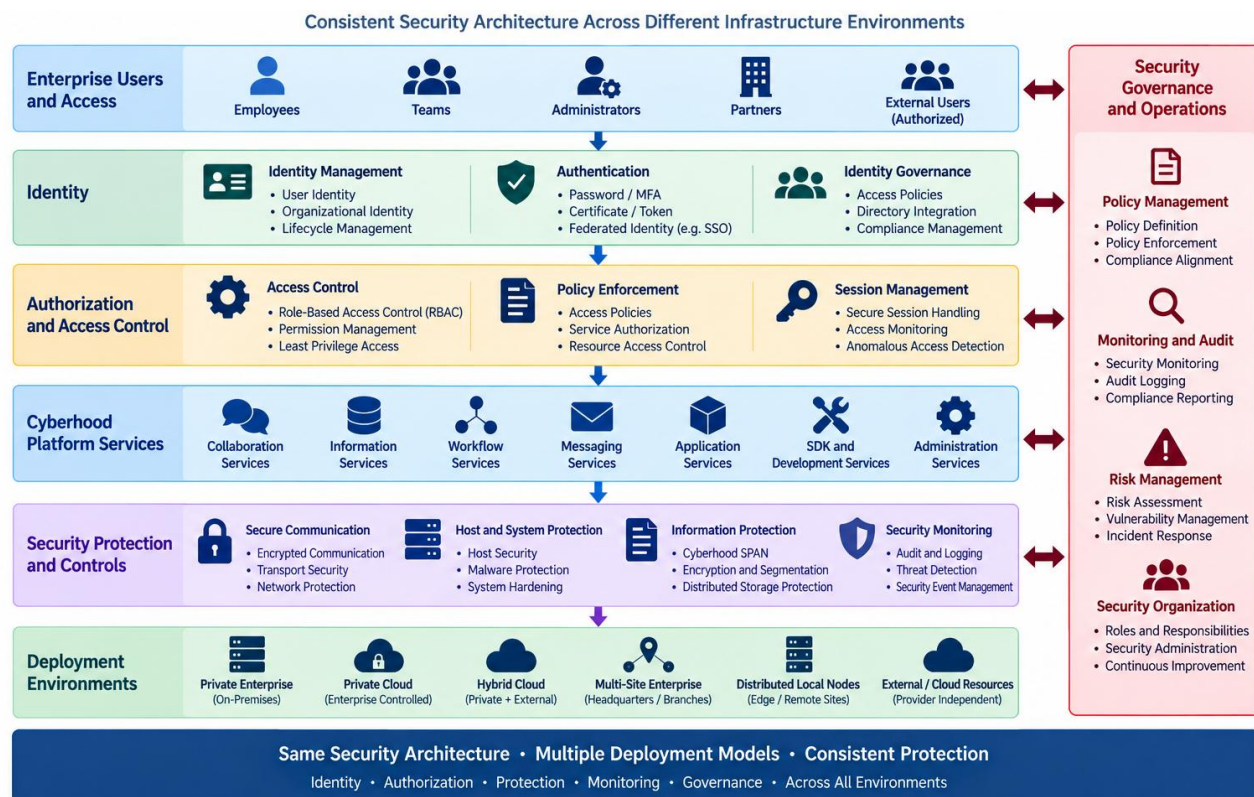


圖 9-6 — 跨部署模式的安全

部署模式改變基礎架構拓撲，但不取代安全架構。

安全政策與部署拓撲彼此相關，但在架構上有所區別。

分散式部署延伸安全邊界，而不是消除安全邊界。

9.13 跨站點企業協作

分散式組織需要不受使用者實體同站限制的協作能力。Cyberhood 提供共同平台，使不同位置的使用者可參與通訊、資訊分享、工作空間、協作及企業資訊服務。

Cyberhood 工作空間架構——包括我的空間（My Space）、公共空間（Public Space）、我分享的空間（Sharing With Space）與分享給我的空間（Shared From Space）——代表的是邏輯資訊環境，而不是實體場地邊界。

工作空間是邏輯資訊環境，而不是實體站點邊界。

使用者位置 ≠ 資訊位置

協作邊界 ≠ 站點邊界

9.14 企業應用部署

Workflow、Project Management、CRM、ERP 等企業應用運作於共同平台架構之上。其業務責任是邏輯應用責任，不應只由單一實體伺服器位置定義。

業務責任各自專業化；平台服務共享。

應用處理可依應用設計與部署設定，與分散式平台資源形成關係。應用責任是邏輯的；執行位置取決於部署設計。

應用責任屬於邏輯層次；執行位置則取決於部署設計。

企業應用架構 ≠ 固定實體伺服器位置

這不代表每一個應用都會在不同資源或站點之間自動遷移。

9.15 Developer Platform 與分散式應用部署

Cyberhood SDK 與 Distributed Application Framework 提供開發基礎，使額外應用可參與分散式企業架構：

應用 → Cyberhood SDK → Distributed Application Framework → 分散式平台服務 → 分散式基礎架構。

身分驗證建立使用者與分散式應用環境的關係；分散式服務選擇可依 Cyberhood 平台模型，將應用執行與適當平台主機建立關聯。應用也可與身分、授權、資訊服務、Workflow、Messaging、儲存及管理服務形成關係。

分散式服務選擇 ≠ 通用的自動應用容錯移轉。

應用擴充應維持平台架構一致性。

9.16 模組化部署擴充

企業需求會持續演進，可能增加運算能力、分散式節點、儲存容量、組織據點或應用能力。Cyberhood 支援這些維度依需求模組化演進。

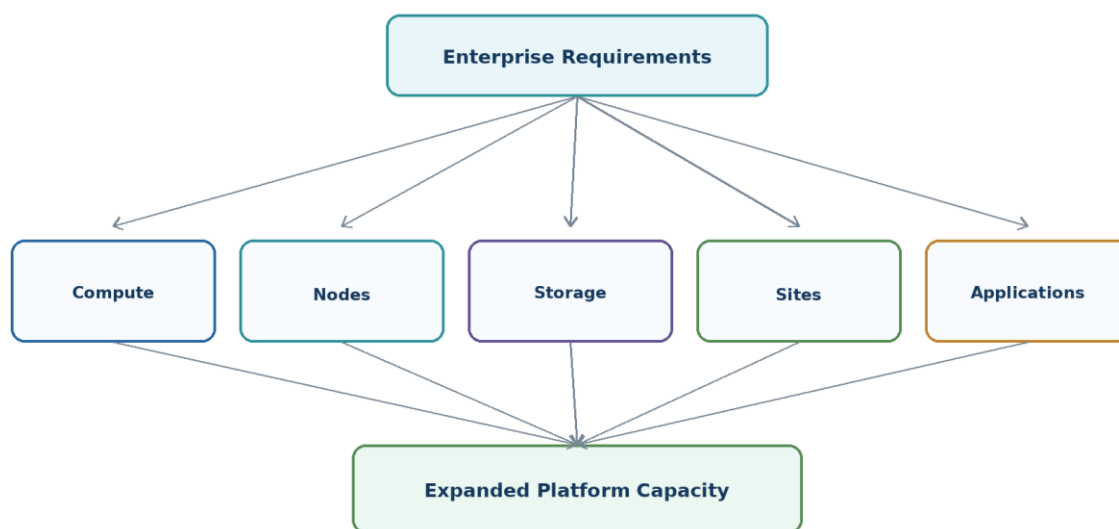


圖 9-7 — 模組化部署擴充模型

模組化擴充是多維度的，而非強制循序路徑：

- 運算擴充 — 增加運算資源。
- 節點擴充 — 增加參與的分散式節點。
- 儲存擴充 — 增加儲存容量，並在適用時增加 SPAN 參與資源。
- 站點擴充 — 增加組織據點或基礎架構位置。
- 應用擴充 — 透過既有或可擴充的平台服務增加應用能力。

擴充會改變容量與拓撲，但不需要重新定義平台的基本架構。

9.17 私有企業參考架構

私有企業參考架構呈現企業控制環境中，企業使用者、企業服務、Cyberhood 平台服務、分散式資源與受保護資訊之間的邏輯關係。它是邏輯參考模型，而非強制硬體配置；節點、儲存、實體系統與服務數量依組織需求決定。

企業服務運作於 Cyberhood 平台服務之上；分散式服務資源與 Cyberhood SPAN Protected Information Layer 可透過彼此相關但不同的架構路徑運作於參與的運算、網路與儲存資源之上。

私有企業部署定義的是控制環境，而不是強制性的實體拓撲。

9.18 多站點企業參考架構

多站點企業參考架構呈現總部、分公司及其他組織位置如何參與共同的邏輯 Cyberhood 平台。各站點可依營運角色配置不同的平台服務、企業應用、DLN、運算、儲存、網路及 SPAN 參與資源。

共同平台架構不要求相同站點架構；

集中協調不要求完全中央集中。

因此，分公司不必只被視為遠端使用單一中央應用環境的使用者；在適當情況下，分散式基礎架構可成為更廣泛企業平台拓撲的一部分。

9.19 混合企業參考架構

混合企業參考架構結合企業自主管理基礎架構、分散式組織站點，以及外部或雲端基礎架構資源。不同來源的資源可參與分散式平台，而 Cyberhood 邏輯架構保持一致。

基礎架構來源 ≠ 平台架構。

基礎架構可以不同；平台架構保持一致。

此架構刻意不依賴特定公有雲供應商。實際的基礎架構整合、網路、安全、營運控制、服務部署與雲端設定，取決於組織所選擇的環境。

9.20 Cyberhood 部署架構模型

完整的 Cyberhood 部署架構整合企業營運、企業服務、共同平台能力、分散式基礎架構、受保護資訊及跨層安全。

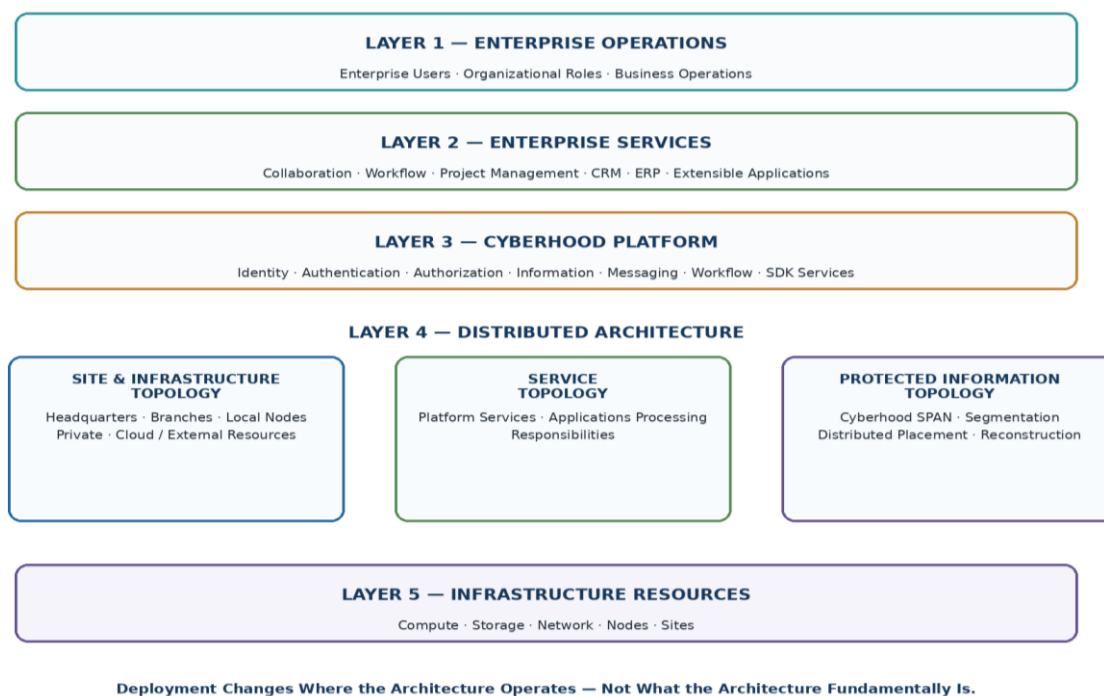


圖 9-8 — Cyberhood 企業部署架構模型

此模型區分站點與基礎架構拓撲、服務拓撲及受保護資訊拓撲。這些維度彼此相關，但各自具有不同的架構責任。安全則透過身分、驗證、授權、安全通訊、主機防護與受保護資源，作為跨層責任貫穿整體架構。

彼此相關 — 但在架構上有所區別

私有企業、私有雲、混合雲、多站點企業、分散式本地節點與復原導向部署，代表 Cyberhood 整體架構因應不同企業基礎架構需求的不同應用方式。

一套平台架構 — 多種部署模式

部署改變架構運作的位置，而不是架構的本質。

關鍵架構原則

- 一套平台架構 — 多種部署模式 — 不同基礎架構環境可參與同一套 Cyberhood 邏輯架構。
- 邏輯架構與實體拓撲有所區別 — 部署拓撲決定資源在哪裡運作；平台架構決定企業能力如何與這些資源形成關係。
- 原生分散式設計 — 運算、儲存、網路、節點、服務、受保護資訊與組織據點，可依部署需求參與分散式架構。
- 共同架構不要求站點完全相同 — 不同組織據點可採用不同的基礎架構與服務責任。
- 集中協調不等於完全中央集中 — 分散式據點可參與整體平台，而不必將架構簡化為僅遠端存取單一中央系統。
- 服務配置與受保護資訊配置有所區別 — 平台或應用服務的運作位置，本身不會定義其完整受保護資訊的所在位置。
- 高可用性與復原服務不同目標 — 高可用性著重維持服務持續性；復原導向架構著重恢復服務。
- 安全延伸至各種部署模式 — 身分、驗證、授權、安全通訊、主機防護、惡意程式防護與資訊保護，在不同部署拓撲中仍持續適用。
- 協作不受實體站點位置限制 — 組織工作空間與協作服務是在站點拓撲之上的邏輯企業環境。
- 應用運作於基礎架構拓撲之上 — 業務應用責任與對單一固定實體基礎架構位置的依賴彼此分離。
- 模組化擴充是多維度的 — 運算、節點、儲存、站點、應用與平台容量可依組織需求演進。
- 部署特性取決於實際設定 — 可用性、復原、效能、安全設定與服務行為，取決於參與的基礎架構、服務、應用與部署設計。

重點摘要

- Cyberhood 不要求單一固定的實體部署拓撲。
- 私有企業、私有雲、混合雲、多站點企業、分散式本地節點與復原導向部署，均可在更廣泛的 Cyberhood 架構中運作。
- 平台架構與實體部署拓撲彼此相關，但仍屬不同的架構責任。
- 站點拓撲、服務拓撲與受保護資訊拓撲，代表不同的架構責任。
- 高可用性提供服務持續性的架構基礎；復原導向架構則處理服務恢復。
- Cyberhood SPAN 在參與的儲存資源之間提供 Protected Information Layer，但不表示服務配置與資訊配置必然相同。
- 安全、協作、企業應用與應用擴充能力，在不同部署模式下仍與共同平台架構保持連結。
- Cyberhood 部署架構可隨基礎架構與組織需求變化而模組化演進。

一套平台架構 — 多種部署模式。

摘要

Cyberhood 的部署模式與參考架構，定義分散式企業平台如何在不同企業基礎架構環境中運作，而不需要採用單一強制性的實體拓撲。

此架構將企業服務、共同平台能力、分散式基礎架構與受保護資訊區分為彼此相關的架構責任。私有企業、私有雲、混合雲、多站點企業、分散式本地節點與復原導向部署，提供依組織需求套用此架構的不同方式。

部署架構中特別重要的三個維度為：站點拓撲定義基礎架構資源存在的位置；服務拓撲定義平台與應用責任運作的位置；受保護資訊拓撲定義受保護企業資訊如何分散。三者彼此相關，但不能互相等同。

應用在某一站點運作，不代表其完整受保護資訊必然位於該站點。分散式受保護資訊不代表應用一定分散執行；地理基礎架構分布也不代表自動 **Active-Active** 運作或自動地理容錯移轉。

Cyberhood 高可用性架構透過分散式資源、故障偵測、隔離、重新分配與復原，提供維持服務持續性的架構基礎。復原導向部署則處理當中斷超過現行環境持續能力後，恢復服務與資訊的不同需求。平台架構本身不定義通用的 RPO、RTO 或自動災難復原政策。

Cyberhood SPAN 透過 Protected Information Layer 延伸部署架構，使邏輯企業資訊可與分散式受保護儲存資源形成關係。安全則持續透過身分、驗證、授權、安全通訊、主機防護、惡意程式防護與受保護資訊，作為跨層架構責任運作。

企業協作與企業應用運作於分散式平台基礎之上；Cyberhood SDK 與 Distributed Application Framework 則提供額外應用能力參與同一整體架構的路徑。

此架構可透過增加運算資源、分散式節點、儲存容量、組織站點與應用能力持續演進，而不需要在概念上替換基本平台模型。

企業需求 → 部署模式 → Cyberhood 平台架構 → 站點 + 服務 + 受保護資訊拓撲 → 分散式基礎架構資源 → 企業營運能力

一套平台架構 — 多種部署模式。

部署改變架構運作的位置，而不是架構的本質。

Cyberhood — 一套平台架構。多種部署模式。為分散式企業營運而打造。

商業價值與企業優勢

執行概述

當基礎架構、資訊、應用、安全與組織流程不再是孤立技術領域，而是在協調一致的環境中運作時，企業科技才能形成可持續價值。企業成長過程中，儲存、通訊、協作、Workflow、CRM、ERP、安全與開發系統逐步增加，雖各自解決合理需求，卻可能造成身分、管理、資訊、安全、基礎架構及營運流程碎片化。

Cyberhood 從企業平台架構角度處理此問題，將分散式基礎架構、共同平台服務、身分與授權、企業安全、受保護資訊、協作、企業應用及應用擴充整合於共同架構環境。其價值因此超越單一產品功能。

架構 → 平台能力 → 營運能力 → 組織價值 → 企業優勢

分散式基礎架構為組織延伸、服務持續性與基礎架構演進提供基礎；共同平台服務在各企業能力之間建立架構一致性；身分與授權則連結人員、組織角色、應用、資訊與受保護資源。

Cyberhood SPAN 提供分散式 Protected Information Layer，旨在降低企業資訊對單一儲存資源的不必要依賴，並支援資訊保護、容錯、重建及保護狀態復原。

協作服務連結人員、通訊、工作空間、企業資訊與組織活動。企業應用則透過 Workflow、Project Management、CRM、ERP 與相關能力支援專業化的業務責任。

Cyberhood SDK 與 Distributed Application Framework 提供可擴充的基礎，使其他應用能力能在共同平台架構中持續開發。

這些能力共同建立一套企業平台，不僅支援目前營運，也提供可隨組織成長、基礎架構變化及未來應用需求持續演進的架構基礎。

架構創造能力。能力支援營運。營運創造商業價值。

10.1 從技術架構到企業價值

技術架構本身不會直接創造企業價值；

當架構能力改善組織營運、資訊保護、人員與流程協調、變更管理及未來需求支援能力時，價值才會形成。

Cyberhood 透過結構化的企業價值進程連結這些關係。



圖 10-1 — 從技術架構到企業優勢

技術架構提供分散式基礎架構、平台服務、身分、安全、受保護資訊、協作、企業應用與 Developer Framework。

平台能力將這些基礎轉化為可重用的身分驗證、授權、資訊保護、協作、Workflow、Messaging、分散式服務與應用整合能力。

營運能力使組織能存取資訊、協調工作、支援分散式使用者、執行業務流程、保護資訊並運作應用。

當這些能力支援一致性、韌性、資訊可用性、協作、治理、適應性與組織協調時，便形成組織價值。

企業優勢代表多項企業能力在共同架構基礎上運作所形成的長期架構效益。

分散式基礎架構 → 分散式營運 → 組織延伸

高可用性架構 → 服務持續性 → 營運韌性

Cyberhood SPAN → 受保護資訊 → 資訊韌性

共同身分與授權 → 一致的存取控制 → 企業治理

協作服務 → 連結人員與資訊 → 組織協調

共同平台 + SDK → 應用擴充性 → 架構演進

科技在架構能力轉化為組織能力時，才具有策略價值。

10.2 降低企業科技碎片化

企業科技通常隨需求逐步增加，最終可能形成彼此分離的通訊、檔案管理、Workflow、Project Management、CRM、ERP、儲存、安全、管理與應用開發環境。問題不一定是功能不足，而是獨立系統在身分、授權、資訊庫、管理、安全控制、基礎架構與應用整合上產生不必要重複。

更多系統 → 更多獨立基礎 → 更高的整合與管理複雜度

Cyberhood 透過共同的分散式企業平台處理此挑戰，使多種企業能力能與共享平台服務形成關係。

不同應用仍持續承擔不同的業務責任。目標不是讓所有應用相同，而是降低在身分、資訊、管理、安全與基礎架構上的不必要重複。

業務責任各自專業化；平台服務共享。

目標不是消除專業化，而是降低不必要的架構碎片化。

10.3 統一企業平台

Cyberhood 被設計為統一企業平台，而非互不相關的基礎架構與應用產品集合。平台連結分散式基礎架構、共同平台服務、身分與授權、企業安全、受保護資訊、協作與資訊服務、企業應用及 Developer Platform。

這些領域在功能上仍各自獨立：CRM 不等於儲存、身分不等於 Workflow、SPAN 不等於 ERP。改變的是它們之間的架構關係。統一架構 ≠ 相同功能。專業化能力 — 共同架構基礎。

這些領域在功能上仍彼此不同。CRM 不會變成儲存；身分不會變成 Workflow；Cyberhood SPAN 也不會變成 ERP。改變的是它們之間的架構關係。

統一架構 ≠ 相同功能

統一平台並非要求所有功能都承擔相同的責任。它提供了一個通用基礎，使各項專業職責能夠以一致的方式互動。

身分驗證可以作為平台功能運行，而不僅僅是應用程式的特定功能。資訊保護可以作為架構層運行，而不僅僅是孤立的儲存功能。協作可以與企業資訊協同運行，而不是作為獨立的通訊環境。應用程式可以運行在通用平台服務之上，而無需為每個新的業務功能建立完全獨立的架構基礎。

專業化能力 — 共同架構基礎

10.4 架構整合與一致性

當每個業務能力都引入獨立架構基礎時，企業科技會愈來愈難協調。

Cyberhood 提供替代模型，使多種企業能力可運作於共享分散式基礎架構與共同平台服務之上。

獨立基礎	共同平台
應用 A → 獨立身分	應用 A · B · C
應用 B → 獨立授權	共同平台服務
應用 C → 獨立基礎架構	分散式基礎架構
重複管理	協調一致的架構關係

圖 10-2 — 從獨立基礎到共同平台

獨立應用基礎 → 共享平台關係 → 更高的架構一致性

架構整合不要求每個工作負載使用相同實體資源。專業系統、特殊基礎架構需求、安全設定與應用責任仍可存在。

目標是降低架構基礎上的不必要重複。隨需求演進，新增資源與能力可加入既有平台，而不是自動形成另一個孤立環境。

這可提升身分、授權、資訊保護、管理、協作及應用整合的一致性。

較少的獨立基礎 — 更高的架構一致性

平台整合不等於功能中央集中。

10.5 業務持續性與營運韌性

現代企業營運依賴數位服務、應用與資訊的持續可用。Cyberhood 透過第 3 章的高可用性架構，結合分散式資源、故障偵測、資源隔離、服務或工作負載重新分配、復原及容量恢復，降低單一元件故障直接造成企業營運中斷的依賴。

從企業角度而言，價值不只是存在備援資源，而是降低單一故障條件對營運的影響。

分散式資源 → 降低依賴 → 服務持續能力 → 營運韌性

高可用性 → 持續營運

復原導向架構 → 恢復營運

業務持續性是服務持續架構所形成的組織成果。

然而，實際持續與復原特性取決於參與服務、部署拓撲、基礎架構設定、資訊架構及組織復原規劃。

分散式架構提供韌性基礎；實際韌性取決於部署設計。

10.6 將資訊保護視為業務保護

企業資訊不是單純儲存資料；文件、專案資訊、客戶紀錄、財務資訊、營運資料、組織知識與流程紀錄直接參與企業活動。資訊不可用、遭入侵、損毀或無法存取，會影響業務流程、客戶關係、組織協調、財務營運與服務持續性。因此，資訊保護應被理解為企業的責任，而不僅僅是儲存的責任。

Cyberhood 將身分、驗證、授權、安全通訊、主機保護、惡意程式防護及 Cyberhood SPAN 連結為分層資訊保護架構。

資訊保護 → 營運保護 → 業務保護

Cyberhood SPAN 透過將邏輯企業資訊與對單一儲存資源的不必要依賴分離，從而發揮其作用。SPAN 透過受保護的分段、加密、分散式部署、容錯、重建、資源隔離和保護狀態復原，在企業資訊服務之下提供受保護的資訊層。在受保護儲存之前進行惡意程式偵測，為資訊生命週期增添了額外的保護階段。該架構並非旨在消除所有資訊風險。相反，它建立了多重保護關係，旨在減少不必要的依賴，並為企業資訊提供多階段的保護。

保護企業資訊，就是保護依賴該資訊的營運。

資訊韌性是營運韌性的先決條件。

10.7 多站點企業的分散式營運

現代組織通常跨多個實體和基礎架構環境運作。總部、分公司、區域設施、營運站點、資料中心、遠端位置和外部基礎架構都可能參與企業營運。

因此，架構挑戰不僅在於如何連接各個位置，更廣泛的挑戰在於如何在這些位置之間維護一致的企業營運環境。

Cyberhood 透過第 9 章中建立的分散式部署模型來滿足這項需求。組織內的各個站點可以在通用平台架構中參與，同時保留符合本地需求的基礎架構和服務職責。

分散式本地節點（DLN）提供了一種機制，可以將 Cyberhood 平台的功能擴展到適當的分散式位置。

分散式位置 → 共同平台架構 → 協調一致的企業營運

目標並非使每個站點的架構完全相同。不同的地點可能需要不同的運算、儲存、網路、平台服務、應用程式或本地資源組合。其價值在於跨越這些差異，維持架構的共通性。

共同企業架構不要求相同的站點基礎架構。

分散式營運不應自動形成分散式科技孤島。

地理分散 → 平台一致性 → 組織協調 → 企業延伸

10.8 企業協作與組織生產力

企業運作依賴人、溝通、資訊、職責和組織流程之間的關係。當這些要素在一個互聯的環境中運作，而不是在孤立的通訊和資訊系統中運作時，協作效率會更高。

Cyberhood 將組織身分與溝通、資訊管理、工作空間、共享、版本控制、搜尋和企業工作協調連結起來。

工作空間包括我的空間、公共空間、我分享的空間與分享給我的空間，代表邏輯資訊環境，而非實體站點位置。

人員 + 通訊 + 資訊 + 協作 → 組織工作

這種架構的價值並非僅僅體現在提供獨立的協作功能上。其意義在於將協作置於與身分和授權、企業資訊、受保護資訊、企業應用和分散式基礎架構相同的更廣泛的平台架構之中。這使得使用者溝通方式、資訊存取和共享方式、組織工作執行方式以及資源保護方式之間實現了連續性。

此架構能夠減少溝通、資訊存取、共享、協作和業務流程之間不必要的割裂，進而提升組織效率。然而，最終的效率提升取決於組織流程、使用者採納率、應用設計、營運實務和部署配置。

協作不只是通訊，而是人員與企業資訊之間的架構關係。

架構基礎	營運能力	企業價值
高可用性（HA）	服務持續性	營運韌性
Cyberhood SPAN	受保護資訊	資訊韌性
多站點架構	協調分散據點	企業延伸能力
協作平台	連結人員與資訊	組織協調

圖 10-3 — 從平台架構到企業營運

10.9 整合式企業應用

企業營運依賴各種應用程式，這些應用程式負責不同的組織和業務職責。Cyberhood 的企業應用生態系統涵蓋工作流程、專案管理、客戶關係管理 (CRM)、企業資源規劃 (ERP) 及相關功能。這些應用程式之所以保持專業化，是因為它們所負責的職責本質上各不相同。Cyberhood 的架構價值並非在於試圖讓這些應用程式完全相同，而是讓專業化的應用程式與通用的企業平台基礎協同運作。

專業化企業應用 → 共享平台基礎 → 整合式企業營運

應用程式可以與身分驗證、授權、資訊服務、協作、工作流程機制、受保護資訊、分散式資源和管理等通用功能協同運作。這降低了每個新業務應用程式都需要建立完全獨立的架構基礎的必要性。

業務責任各自專業化；平台服務共享。

應用整合不等於功能融合。

10.10 共同身分、授權與企業治理

身分不只是登入機制；在企業平台中，它建立人員、組織角色、應用、資訊、權限與企業資源之間的關係。

身分 → 驗證 → 授權 → 企業資源

從企業角度而言，此架構為協作、資訊存取、企業應用及分散式應用服務建立治理基礎。

身分 → 角色 → 權限 → 資源 → 活動

這提供架構基礎，用以判斷並決定誰正在與平台互動、其組織角色為何、可存取哪些資源，以及何種活動可以被執行。

僅靠身分和授權並不能建立完整的企業治理或合規架構。治理還取決於組織政策、管理程序、應用程式設計、安全控制和營運監督。然而，共同的身分和授權提供了一個一致的架構基礎，使這些治理職責得以有效運作。

共同身分 → 一致授權 → 協調一致的資源治理

身分將組織連結至技術架構。

10.11 企業資訊生命週期價值

企業資訊在其整個生命週期中不斷演變。它可以被創建、儲存、共享、協作、版本控制、搜尋、重複使用、保護，並融入組織流程中。

建立 → 儲存 → 分享 → 協作 → 版本化 → 搜尋 → 保護

資訊只有在以下情況下才能創造組織價值：授權使用者可存取資訊、需要時可尋找資訊、可在協作和應用程式中使用訊息，並受到適當保護。

此生命週期的重要性在於，Cyberhood 不只將企業資訊視為儲存裝置上的檔案，而是視為跨協作、應用、安全與組織流程參與的企業資源。

人員 + 協作 + 應用 + 安全 + 組織流程

資訊 → 可存取性 → 協作 → 重複使用 → 保護 → 組織知識

儲存保存資訊；資訊生命週期則從資訊創造組織價值。

企業資訊的價值不只取決於其存在，也取決於可用性、可發現性、授權使用與保護。

資訊生命週期管理與資訊保護是互補責任。

10.12 安全、治理與架構一致性

當身分、授權、安全、資訊、基礎架構與管理分散於許多互不相關的環境時，企業科技複雜度會提高。更大的問題不是系統數量，而是組織必須協調多少獨立架構關係。

Cyberhood 透過共同平台架構，使身分驗證、授權、資訊服務、分散式儲存、Workflow、Messaging、SDK 服務、管理、安全與受保護資訊彼此形成關係。安全跨越身分、驗證、授權、安全通訊、主機保護、惡意程式防護及受保護資訊等多層。

較少的獨立基礎 → 更高的平台一致性 → 更協調的治理

安全運作跨越多個層面，包括身分識別、身分驗證、授權、安全通訊、主機保護、惡意程式防護和資訊保護。

通用平台架構的目的並非在於讓企業 IT 維運變得簡單。分散式企業環境依然複雜，需要相應的規劃、架構、管理、配置、監控、維護和安全策略。

其價值在於架構的一致性。

架構一致性可降低獨立技術基礎之間不必要的協調成本。

營運簡單化不是目標；協調一致的架構才是。

10.13 模組化成長與架構投資保護

企業技術需求不斷演變。組織可能會增加使用者、應用程式、運算資源、儲存容量、分散式節點、業務功能和組織站點。

Cyberhood 透過模組化分散式架構來應對這種演進。成長可以發生在運算、分散式節點、儲存、站點、平台容量和應用程式等各個方面。這些維度無需按特定順序擴展。組織可以在不新建站點的情況下增加儲存容量，在不取代整個基礎架構的情況下引入新應用程式，或根據營運需求將平台擴展到新的組織位置。

模組化擴充 → 架構連續性 → 降低根本性平台替換需求

架構投資保護並不意味著基礎架構永遠不需要更換，技術永遠不會過時，或擴展無需額外成本。它的意義是，即使基礎架構、應用程式和組織需求不斷演變，通用平台模型也能保持其效能。

投資保護更應理解為架構連續性，而非技術永久性。

10.14 支援組織成長

組織的發展會從根本上改變技術需求，而這種改變遠不止於基礎架構的承載能力。企業可能會增加員工、設立部門、開設分支機構、引入新的業務流程、增加資訊量、部署更多應用程式，或擴展到地理分散式營運。

Cyberhood 的設計旨在使這些變化能夠在更廣泛的分散式平台模型中持續進行。

初始組織 → 增加人員 → 增加流程 → 增加應用 → 增加站點 → 增加企業複雜度

在這演變過程中，分散式基礎架構、通用平台服務、資訊、協作、企業應用和業務營運之間的基本關係始終至關重要。因此，其價值遠不止於硬體可擴展性。

組織成長不需要在每個階段都重新建立企業架構概念。

組織成長應擴展平台，而不是碎片化架構。

10.15 應用擴充性與未來需求

企業需求並非一成不變。隨著組織的演進，新的流程、服務、整合、資訊流和應用需求不斷湧現。

Cyberhood SDK 和分散式應用程式框架提供了一個架構基礎，在此基礎上，可以基於通用平台開發額外的應用功能。

目前應用 + 未來應用 → 共同平台基礎

根據應用程式設計，新應用程式可以與身分驗證、授權、分散式服務、資訊、工作流程、訊息傳遞、受保護資源和管理等通用功能協同運作。因此，該平台在概念上並不局限於某一特定時間點可用的應用程式。然而，可擴展性並不意味著未來的所有應用程式需求都會自動被滿足。其價值在於提供一個基礎，在此基礎上可以開發額外的應用程式功能。

擴充性不是預測未來需求，而是提供回應未來需求的架構。

10.16 降低應用與基礎架構孤島

企業軟體中功能專業化不可或缺。CRM 和 ERP 分別負責不同的業務職責。工作流程管理和專案管理支援不同的組織流程。協作管理和資訊管理滿足不同的使用者和資訊需求。

當功能專業化自動造成平台隔離和基礎架構孤島時，就會出現架構問題。Cyberhood 將這些概念分離出來。應用程式可以在保留其專業業務職責的同時，根據需要參與到與身分、授權、資訊、工作流程、訊息傳遞、儲存、管理、受保護資訊和分散式基礎架構的通用關係中。

專業化應存在於業務層，而不必在每一技術層都形成架構隔離。

業務責任各自專業化；平台服務共享。

這可降低每個新應用都必須建立完全獨立技術基礎的架構壓力。

10.17 管理可視性與營運監督

企業治理不僅需要制定資源存取規則，還需要對企業服務的使用進行管理可見性。

Cyberhood 提供包括組織身分、授權、資源權限、管理和活動記錄在內的架構元素，這些元素有助於實現營運監督。

身分 → 角色 → 權限 → 資源 → 活動

在此模型中，活動資訊可以支援管理監督、營運審查和組織監管。這些功能不應被解讀為構成適用於所有產業的完整監管合規、審計或治理架構。它們提供的是平台級機制，組織可以將其融入更廣泛的治理和管理實踐中。

治理規則 → 授權活動 → 管理可視性

治理定義關係；可視性協助組織觀察其實際運作。

10.18 長期架構彈性

企業科技決策具有長期影響：基礎架構改變、組織擴張、應用演進、資訊量增加、安全需求發展、新流程出現。Cyberhood 透過架構責任分離處理此挑戰。

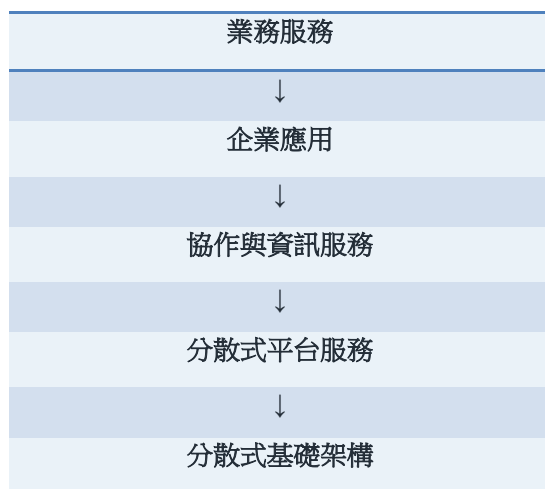


圖 10-4 — Cyberhood 分層架構連續性

這種分層模型並非意味著每一層都可以獨立更改而無需整合或維運工作。相反，它建立了架構職責之間的概念分離。

可以引入額外的基礎架構。可以開發新的應用程式。可以加入新的組織站點。資訊和協作服務可以在更廣泛的平台模型中繼續運作。

架構演進應延伸平台，而不是不必要地取代其基本關係。

技術會改變；架構關係提供連續性。

10.19 Cyberhood 企業價值模型

Cyberhood 的企業價值不是來自單一能力，而是來自各架構層之間的協調關係。

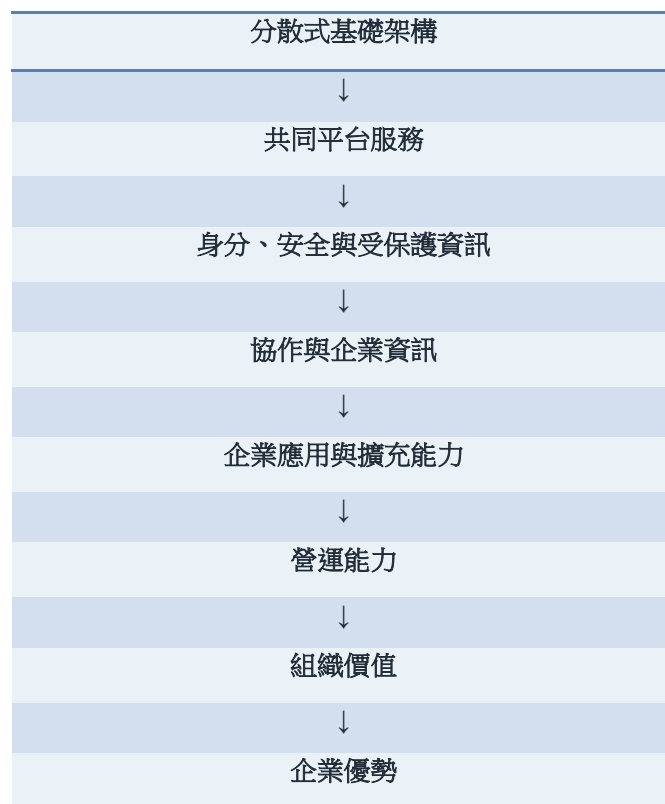


圖 10-5 — Cyberhood 企業價值模型

分散式基礎架構提供技術基礎。通用平台服務建立身分、授權、資訊、通訊、管理、工作流程和分散式服務之間的共享關係。

安全性和 Cyberhood SPAN 保護企業使用者、服務、資源和資訊之間的關係。協作和資訊服務將人員與組織資訊和工作連結起來。

企業應用程式將通用平台功能轉化為專門的業務流程。Cyberhood SDK 擴展了此架構，使其能夠支援未來的應用程式功能。

這些架構元素構成了營運能力。當平台支援連續性、資訊韌性、協作、治理、分散式營運和組織發展時，營運能力就能創造組織價值。

架構 → 能力 → 營運 → 組織價值 → 企業優勢

Cyberhood 的價值不是由單一能力定義，而是由連結這些能力的架構定義。

10.20 策略性企業優勢

Cyberhood 分散式企業平台建立一組源自各架構層相互關係的策略性企業優勢。

- 統一企業架構 — 基礎架構、平台服務、資訊、安全、協作、應用與擴充性在協調一致的框架中共同參與。
- 分散式企業營運 — 總部、分公司、區域設施及其他參與環境可在共同的分散式平台模型中運作。
- 資訊韌性 — 多層安全控制與 Cyberhood SPAN Protected Information Layer 形成關係。
- 營運韌性 — 分散式基礎架構與高可用性為服務持續性提供基礎，而復原導向架構則支援服務恢復。
- 整合式協作 — 人員、通訊、資訊、分享、工作空間、搜尋與組織工作在共同平台中形成關係。
- 整合式企業應用 — Workflow、Project Management、CRM、ERP 與相關應用保留專業業務責任，同時共享共同平台能力。
- 應用擴充性 — Cyberhood SDK 與 Distributed Application Framework 為其他應用開發提供架構基礎。
- 模組化演進 — 運算、儲存、節點、站點及應用能力可依組織需求持續演進。
- 長期架構一致性 — 隨組織演進，基礎架構、平台服務、資訊、應用與業務營運之間的基本關係仍可持續有效。

因此，Cyberhood 的定位不只是技術集合，而是分散式企業營運與長期組織演進的架構基礎。

關鍵架構原則

- 架構優先於碎片化 — 企業能力應在協調一致的架構關係中運作，而不是每次新增能力就自動引入獨立技術基礎。
- 共享平台基礎 — 身分、授權、資訊、通訊、管理、受保護資源及分散式基礎架構提供可重用的平台能力。
- 業務責任各自專業化；平台服務共享 — 應用保留專業化業務責任，同時參與共同平台基礎。
- 企業應用整合 — API Integration、Transaction Orchestration、ESB、Message Bus、Automatic Cross-Application Synchronization 與共享工作流程連接專業化應用，而不要求功能趨同。
- 資訊作為企業資產 — 企業資訊參與協作、應用、搜尋、安全、治理與業務流程。
- 原生分散式設計 — 企業資源與組織站點可參與更廣泛的分散式架構。
- 以架構實現安全與治理 — 身分、授權、安全通訊、主機保護、受保護資訊、資源權限與管理可視性作為彼此相關的架構責任運作。
- 以架構支援持續性 — 分散式資源、高可用性機制與復原導向架構為服務持續與恢復提供基礎。
- 擴充性作為平台能力 — Cyberhood SDK 使平台架構能超越固定的應用集合持續擴充。
- 模組化演進 — 基礎架構、儲存、站點、應用與平台容量可依組織需求演進。
- 長期架構一致性 — 企業可持續成長，同時維持基礎架構、平台服務、資訊、應用與業務能力之間的基本關係。

企業重點摘要

- Cyberhood 將分散式技術架構與企業營運能力連結。
- 共同平台架構可降低基礎架構、資訊、安全、協作與應用之間不必要的碎片化。
- 高可用性與復原導向架構分別為服務持續與恢復提供互補的架構基礎。
- Cyberhood SPAN 將受保護資訊定位為整體企業架構的一部分，而不是孤立的儲存功能。
- 共同身分與授權為一致的資源治理提供基礎。
- 協作連結人員、通訊、企業資訊與組織工作。
- 專業化企業應用可保留其業務責任，同時共享共同平台服務。
- Cyberhood SDK 與模組化架構為組織及應用演進提供基礎。
- Cyberhood 的策略價值來自分散式基礎架構、受保護資訊、協作、企業應用、治理與擴充性之間協調一致的關係。

架構創造能力。能力支援營運。營運創造商業價值。

摘要

Cyberhood 分散式企業平台的商業價值，來自基礎架構、平台服務、受保護資訊、協作、企業應用、安全、治理與應用擴充性之間協調一致的關係。

分散式基礎架構為不同位置與部署環境提供技術基礎；共同平台服務則在身分、授權、資訊、通訊、管理、Workflow、儲存、應用及分散式資源之間建立一致的關係。

Cyberhood 高可用性架構為服務持續性提供基礎，而復原導向架構則處理較重大中斷後的服務恢復。

Cyberhood SPAN 透過分散式分段、加密、配置、設定式容錯、重建與保護狀態復原，提供 Protected Information Layer。

企業協作連結人員與通訊、工作空間、資訊分享、搜尋及組織活動；Workflow、Project Management、CRM、ERP 與相關企業應用則將平台能力轉化為專業化組織流程。

身分與授權連結人員及組織角色與企業資源；管理可視性與活動紀錄則可支援治理與營運監督。

Cyberhood SDK 與 Distributed Application Framework 使架構超越固定的應用集合，並為其他應用開發提供基礎。

模組化擴充使運算資源、儲存資源、分散式節點、組織站點及應用能力可隨需求變化而演進。

**分散式基礎架構 → 共同平台服務 → 安全與受保護資訊 → 企業整合服務 → 協作與企業資訊
→ 整合式企業應用 → 協調式企業流程 → 業務營運**

目標不只是提供更多科技，而是建立一套架構基礎，使企業科技在基礎架構、資訊、應用、安全需求與組織營運持續演進時，仍能維持協調一致。

架構創造能力。能力支援營運。營運創造商業價值。

Cyberhood — 從分散式架構到可持續的企業能力。

企業應用整合作為組織價值

企業應用整合的價值，在於連接專業化業務責任，而不要求功能趨同。ERP、CRM、EIP、專案管理、工作流程／電子簽核、通訊與協作及其他應用，可依各自業務角色持續演進，同時參與協調一致的企業流程。

API 整合連接應用功能與資訊；交易編排協調跨越應用邊界的活動；工作流程整合組織程序；訊息與服務整合連接參與系統；跨應用自動同步維持相關資訊與流程狀態關係。這些能力共同支援組織協調與營運可視性。

因此，平台整合不代表功能集中化。Cyberhood 透過共同的整合與平台關係，降低架構碎片化，同時保留專業化應用的責任。

應用整合 → 交易編排 → 流程整合 → 資訊同步 → 組織協調 → 營運可視性 → 企業治理

應用整合不等於功能趨同。

平台整合不等於功能集中化。

第 11 章

結論與架構願景

執行概述

企業科技持續在基礎架構、資訊、安全、協作、應用與組織營運等面向演進。

隨著新需求出現，企業經常透過新增系統、新增基礎架構、新增安全機制、新增資訊儲存環境與新增應用來因應。每一項新增項目都可能解決當下需求，但長期下來，組織可能日益依賴一組彼此獨立設計的科技環境。

Cyberhood 提出不同的架構方法。

Cyberhood 分散式企業平台的設計原則，是讓企業科技以協調一致的架構運作，而不是持續累積彼此孤立的系統。

其架構連結分散式基礎架構、共用平台服務、身分與授權、企業安全、受保護資訊、協作與資訊服務、企業應用，以及可擴充的 Developer Platform。

這些能力在功能上仍各自專業化，但共同參與於同一個架構環境。

因此，Cyberhood 的重要性不僅在於個別技術所提供的能力，更在於這些技術之間所建立的關係。

基礎架構 → 平台服務 → 企業能力 → 業務營運

Cyberhood 將此關係延伸至分散式組織環境，同時讓身分、資訊、安全、協作、應用與平台服務維持為彼此相關的架構責任。

Cyberhood 並非由其所包含的技術來定義，而是由連結這些技術的架構所定義。

由此形成的願景，是一個既能支援目前組織需求，又能為持續演進提供架構基礎的企業平台。

11.1 從個別系統到分散式企業平台

企業科技環境很少一開始就是統一架構，而是隨時間逐步演進。

組織導入儲存系統管理資訊、通訊系統連結使用者、工作流程應用協調流程、CRM 管理客戶關係、ERP 支援企業營運、安全技術保護資源，以及基礎架構平台支援應用。

每項技術都有其合理責任。當每一項新責任都導入另一套獨立基礎時，架構挑戰便隨之產生。

因此，功能成長長期可能轉化為架構碎片化。

Cyberhood 從相反方向思考企業科技。它不是先從個別產品出發，再嘗試事後整合，而是先建立分散式平台架構，讓不同企業能力在其中參與。

這並不表示所有企業能力都變成同一個應用。Workflow 仍是 Workflow，CRM 仍是 CRM，ERP 仍是 ERP，協作仍是協作；安全與受保護資訊也仍是不同的架構責任。

改變的是這些能力參與企業環境時所依循的架構基礎。

目標不是消除專業化技術，而是避免專業化自動演變成架構孤島。

新需求 → 新系統 → 新基礎架構 → 新身分體系 → 新資訊環境 → 新管理責任

個別系統 → 共用平台關係 → 分散式企業平台

平台優先於產品

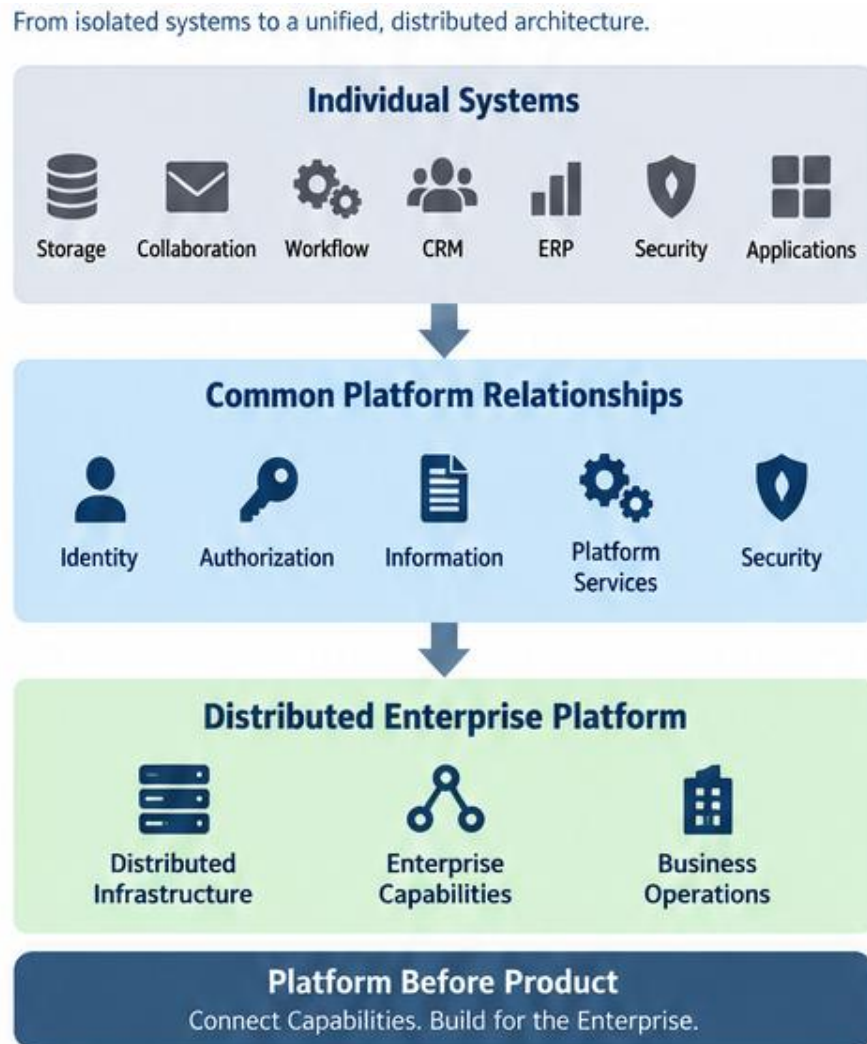


圖 11-1 — 從個別系統到分散式企業平台

11.2 統一的架構基礎

統一企業平台並不要求每一項科技能力執行相同功能，而是要求不同能力在明確定義的架構關係中運作。

Cyberhood 透過分層式企業架構建立這些關係。

分散式基礎架構提供平台所需的運算、儲存、網路、分散式節點及其他參與式基礎架構資源。

分散式平台服務提供共用架構能力，使較高層級的企業服務可與分散式資源建立運作關係。

協作與資訊服務將組織使用者與通訊、工作空間、資訊分享、版本管理、搜尋及受保護資訊服務連結。

企業應用將平台能力轉化為專業化組織功能，例如 Workflow、Project Management、CRM、ERP 及相關企業應用。

業務服務代表最終由科技架構所支援的組織活動與責任。

各層在維持架構關係的同時建立責任分離。業務應用可保持專業化並使用共用平台能力；資訊可跨協作與應用參與，同時持續與授權及保護機制相連；基礎架構可持續演進，而較高層級的架構責任仍維持概念一致性。

統一架構不應與單體式架構混為一談。Cyberhood 統一的是架構關係，同時保留分散式資源、專業化責任與模組化部署。

業務服務 → 企業應用 → 協作與資訊服務 → 分散式平台服務 → 分散式基礎架構

責任分離不代表架構必須分離。

不同責任 — 共同架構基礎

統一架構 ≠ 單體式架構

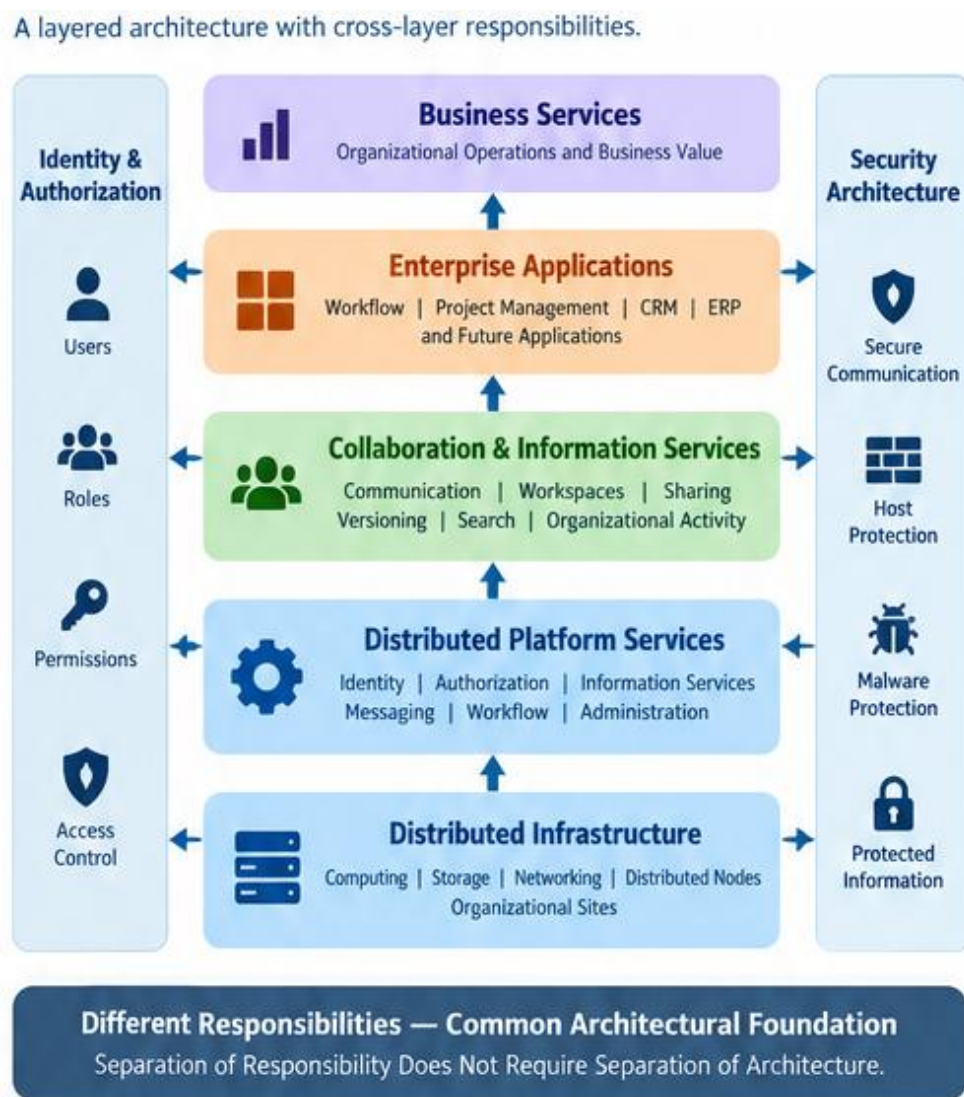


圖 11-2 — Cyberhood 統一架構基礎

11.3 原生分散式設計

Cyberhood 的分散式概念並不限於伺服器的實體配置，而是一項更廣泛的架構特性。

企業使用者、組織站點、運算資源、儲存資源、應用、服務與受保護資訊，都可跨不同基礎架構環境參與。

因此，Cyberhood 將分散式視為平台架構的一部分，而不是平台完成後才額外加入的例外機制。

此分散式模型涵蓋 Master Node、Slave Node、分散式本地節點（Distributed Local Node, DLN）、運算資源、儲存資源、網路資源與組織站點之間的關係。這些資源可依部署需求參與更廣泛的 Cyberhood 環境。

分散式並非為了分散本身，而是為企業韌性、多站點營運、資源參與、受保護資訊配置與模組化成長提供架構基礎。

Cyberhood 不假設每一項企業能力都必須依賴單一伺服器、單一儲存裝置或單一組織位置。

同時，分散式也不應被解讀為自動高可用性、自動地理容錯移轉或全面複寫。實際的服務持續性、服務配置、受保護資訊配置與復原行為，取決於架構與部署設定。

企業分散式架構也存在於多個面向。基礎架構拓樸、服務拓樸、受保護資訊拓樸與組織站點拓樸彼此相關，但在架構上各自獨立。

分散式資源 → 降低依賴

分散式節點 → 跨基礎架構的服務參與

分散式站點 → 多站點企業營運

分散式受保護資訊 → 資訊韌性

模組化資源 → 架構演進

原生分散式設計

分散式架構創造架構上的可能性；部署設計決定實際營運行為。

11.4 資訊作為企業資產

企業資訊是組織中最具持續性的資源之一。基礎架構可以更換、應用可以演進、裝置可以改變、組織結構可以重整，但企業資訊往往會跨越這些變化持續存在。

文件、客戶紀錄、專案資訊、營運資料、財務資訊、流程紀錄、通訊內容與組織知識，不只是被儲存的檔案，而是直接參與企業營運。

因此，Cyberhood 將資訊視為企業資產，而不只是存在於儲存裝置上的資料。在整個生命週期中，企業資訊會與身分、授權、協作、應用、安全及受保護儲存互動。Cyberhood SPAN 進一步將邏輯受保護資訊與對個別儲存資源的不必要依賴分離。因此，不應只透過受保護元件所在的實體裝置來理解一個邏輯企業資訊物件。

邏輯企業資訊不應僅由實體拓樸所定義。資訊保護同時包含兩種彼此相關但不同的關係。存取控制關係處理誰可以存取企業資訊；受保護資訊關係則處理受保護資訊如何跨分散式儲存資源運作。

檔案儲存在哪裡？ → 企業資訊如何參與組織運作？

建立 → 儲存 → 分享 → 協作 → 版本化 → 搜尋 → 保護

身分 → 授權資訊存取 → 協作 → 應用 → 組織知識

資訊是邏輯企業資源；儲存是基礎架構資源。

儲存位置 ≠ 資訊身分

應用位置 ≠ 完整資訊位置

使用者位置 ≠ 資訊位置

身分 → 驗證 → 授權 → 受保護資訊

分段 → 加密 → 分散 → 重建 → 復原

資訊保護同時是存取控制責任，也是資訊架構責任。

11.5 安全即架構

企業安全不能被簡化為單一產品、裝置、網路邊界或控制點。

使用者存取應用，應用存取資訊，資訊跨網路移動，基礎架構承載服務，組織角色建立責任；每一種關係都會產生安全需求。

因此，Cyberhood 將安全視為跨平台運作的架構責任。

身分建立誰正在與企業環境互動；驗證確認該身分是否可被驗證；授權依組織角色與權限決定可使用的資源與動作；受保護資源則代表由這些關係所治理的資訊、應用、服務與平台能力。

其他架構保護機制包括安全通訊、針對分散式主機的 Independent Firewall 保護、惡意程式防護，以及 Cyberhood SPAN 受保護分散式資訊儲存。

這些機制分別處理不同責任。任何單一機制都不應被解讀為可以消除所有安全風險。架構目標是在彼此相關的企業資源與服務之間建立分層保護。

因此，安全是一項跨層責任，而不是獨立的應用層。

身分 → 驗證 → 授權 → 受保護資源

身分安全 + 通訊安全 + 主機保護 + 資訊保護 → 企業安全架構

安全不是單一邊界，而是跨越架構各層的關係。

安全控制保護元件；安全架構保護關係。

11.6 協作作為平台能力

組織透過人員、資訊、通訊、責任與業務流程之間的關係運作。因此，企業協作不能只被視為訊息傳遞或通訊。通訊可以啟動工作，但企業協作還依賴資訊存取、共享情境、組織角色、應用與業務流程。

因此，Cyberhood 將協作定位為原生平台能力。

Enterprise Mail 與 Enterprise Messenger 支援組織通訊；檔案管理、版本控制、全文搜尋、分享與跨平台存取則將使用者與企業資訊連結。

工作空間模型 — 我的空間（My Space）、公共空間（Public Space）、我分享的空間（Sharing With Space）與分享給我的空間（Shared From Space）— 用來組織使用者與組織參與者之間的邏輯資訊關係。

此模型的重要性在於協作並未與更廣泛的平台隔離，而是與身分及授權、企業資訊、受保護資訊、企業應用與分散式基礎架構建立關係。

人員 + 身分 + 通訊 + 資訊 + 業務流程 → 企業協作

協作是人員與企業資訊之間的平台關係。

通訊連結人員；協作連結人員、資訊與工作。

11.7 應用作為平台的一部分

企業應用承擔專業化業務責任。Workflow 支援結構化流程與簽核；Project Management 支援專案導向活動；CRM 支援客戶關係、服務活動、互動歷程及相關資訊；ERP 則支援更廣泛的企業營運領域，包括銷售、採購、會計、資產、庫存、製造、人力資源、預算及相關流程。

這些應用構成 Cyberhood 企業應用生態系統與整合。

然而，Cyberhood 的架構模型並不受限於固定的一組預先定義應用。

Cyberhood SDK 與 Distributed Application Framework 提供基礎，使其他應用可在與分散式平台服務及企業資源建立關係的前提下進行開發。

應用仍負責專業化業務邏輯；平台則依應用設計提供共用架構關係，包括身分、授權、資訊服務、協作、分散式服務、受保護資源與基礎架構存取。

既有應用 + 未來應用 → 共用分散式平台

應用是專業化業務能力；平台是共享的架構基礎。

應用參與平台，但不定義平台。

11.8 一個平台架構 — 多種部署模式

企業組織運作於不同的基礎架構條件。有些維持私有控制的基礎架構，有些採用私有雲環境，有些結合私有與外部基礎架構；許多企業則跨總部、分公司、區域設施或其他分散式組織位置營運。以復原為導向的基礎架構也可參與更廣泛的企業架構。

Cyberhood 不要求這些組織採用完全相同的實體拓樸，而是將邏輯架構與實體部署拓樸分離。

邏輯架構定義基礎架構、平台服務、資訊、應用與業務能力之間的關係；實體部署則依組織需求決定參與資源、服務與資訊的配置位置。

本白皮書建立部署模式包括私有企業、私有雲、混合雲、多站點企業、分散式本地節點（DLN）及復原導向部署。因此，不同部署模式可套用同一個更廣泛的平台架構，而不需要完全相同的基礎架構。

基礎架構 → 平台服務 → 資訊 → 應用 → 業務能力

一個平台架構 — 多種部署模式

邏輯一致性不要求實體一致。

部署改變架構運作的位置，而不是架構本質。

11.9 業務責任各自專業化；平台服務共享

企業應用應依其所支援的業務責任維持專業化。CRM 應處理客戶相關責任；ERP 應處理企業資源與營運責任；Workflow 應處理結構化組織流程；Project Management 應處理專案導向活動；協作服務則應支援組織通訊與資訊關係。

Cyberhood 並不試圖消除這些差異，而是透過架構將業務責任與平台責任分離。

業務應用保留專業化功能；平台服務則依需要提供可重複使用的架構能力，例如身分、授權、資訊服務、通訊、工作流程機制、管理、受保護資訊及分散式基礎架構服務。

此模型讓專業化與架構一致性能夠並存，也避免假設每一個專業化應用都必須導入一套完全獨立的科技基礎。

業務責任各自專業化；平台服務共享。

專業化應用 → 共用平台服務 → 共同分散式基礎架構

專業化創造業務價值；共享平台服務維持架構一致性。

平台應標準化共同關係，而不是標準化每一項業務功能。

Specialized applications, shared platform services, common infrastructure.

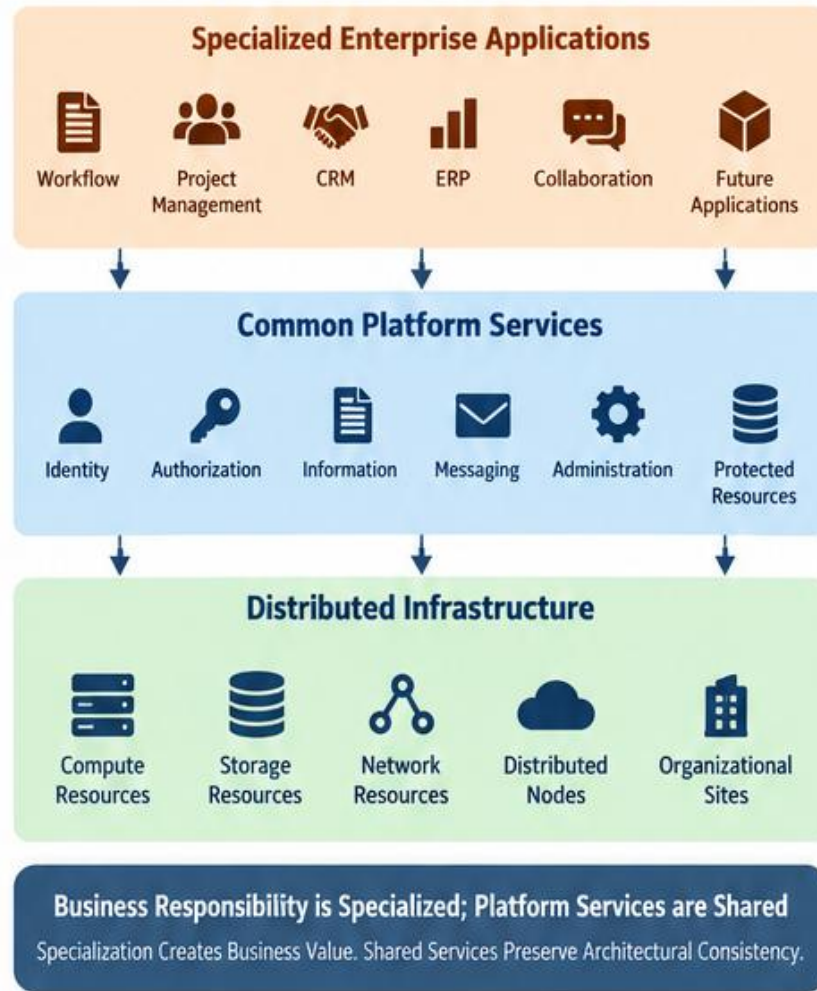


圖 11-3 — 共享平台上的專業化企業能力

11.10 持續演進的架構

企業需求持續演進。組織增加使用者、資訊量持續成長、新應用被導入、基礎架構容量改變、新增組織據點、安全需求演進，業務流程也持續重新設計。

因此，可持續的企業架構必須支援變化，而不是每當新需求出現時，都要求組織在概念上重新建構整個科技環境。

Cyberhood 透過四項互補的架構特性因應此需求：分層式架構、分散式基礎架構、模組化演進與應用擴充性。這些特性共同使平台能跨基礎架構、資訊、應用與組織需求持續演進，同時保留共同的概念基礎。額外的運算或儲存資源可加入分散式環境；分散式本地節點（DLN）可將平台延伸至其他組織位置；企業應用可因應新增或改變的業務流程；Cyberhood SDK 與 Distributed Application Framework 則為其他應用能力提供開發基礎。

目標不是科技永久不變。個別產品、基礎架構資源與實作細節都會持續改變；架構目標是在變化中維持連續性。

目前需求 → 模組化變更 → 擴充能力 → 持續演進的企業平台

科技會改變，業務需求會演進，架構關係提供連續性。

可持續的架構，是能吸收變化而不失去一致性的架構。

11.11 Cyberhood 架構願景

Cyberhood 的架構願景整合了本白皮書所建立的主要關係。

在基礎架構層，分散式資源提供技術基礎；在平台層，共用服務為身分、授權、資訊、通訊、工作流程、管理、分散式處理與應用參與建立可重複使用的關係。

在協作與資訊層，人員與企業資訊、通訊、工作空間、分享、搜尋及組織活動互動；在應用層，專業化企業系統將平台能力轉化為業務流程；在業務層，這些流程支援企業營運。

安全跨越這些層級運作。受保護資訊與身分、授權、協作、應用及分散式儲存資源建立關係。部署模式決定架構實際運作的位置，但不重新定義其基本邏輯關係。

因此，Cyberhood 模型的意義並非功能一致化。基礎架構仍是基礎架構，安全仍是安全，協作仍是協作，應用保留專業化責任，資訊則維持為邏輯企業資源。

Cyberhood 所提供的，是讓這些責任能共同參與協調一致企業環境的架構。

分散式基礎架構 → 共用平台服務 → 協作與資訊服務 → 企業應用 → 業務服務

一套分散式企業架構，在同一個協調一致的平台環境中連結基礎架構、資訊、安全、協作、應用與業務營運。

整合不要求一致化。

協調不要求中央集中。

A distributed enterprise architecture connecting all key components.



圖 11-4 — Cyberhood 架構願景

11.12 Cyberhood 架構原則

1. 原生分散式設計 — 分散式基礎架構是平台基礎的一部分，而不是選配延伸。分散式是一項架構特性，而不只是部署選擇。
2. 平台優先於產品 — 個別功能與應用參與更廣泛的企業平台架構。平台定義關係，產品承擔專業化責任。
3. 身分作為基礎 — 身分連結使用者、組織角色、授權、應用、資訊與企業資源。身分將組織與科技架構連結。
4. 資訊作為企業資產 — 企業資訊跨儲存、協作、搜尋、應用、安全與組織流程參與。資訊是邏輯企業資源；儲存是基礎架構資源。
5. 安全由架構建立 — 安全跨身分、授權、安全通訊、主機保護、惡意程式防護與受保護資訊運作。安全不是單一邊界，而是跨越架構各層的關係。

6. 協作作為原生能力 — 通訊、資訊、分享、工作空間與組織互動共同參與平台。協作連結人員、資訊與工作。
7. 業務責任各自專業化；平台服務共享 — 應用保留專業化業務責任，同時與共用平台能力建立運作關係。專業化與架構一致性可以並存。
8. 一個平台架構 — 多種部署模式 — 不同實體環境可套用同一個更廣泛的邏輯平台架構。邏輯一致性不要求實體一致。
9. 模組化演進 — 運算、儲存、分散式節點、組織位置與平台容量可隨企業需求改變而演進。成長應延伸架構，而不是使架構碎片化。
10. 面向未來開發的擴充性 — **Cyberhood SDK 與 Distributed Application Framework** 為其他應用能力提供基礎。擴充性不是預測未來需求，而是提供回應未來需求的架構。

這些原則共同定義 Cyberhood：它不是固定的科技配置，而是支援分散式企業運算與組織持續演進的架構框架。

最終架構宣言

科技會演進，架構得以延續。

企業科技將持續改變。

基礎架構將更加分散，資訊量將持續成長，安全需求將持續演進，組織也會導入新的應用、流程、據點與營運模式。

因此，長期挑戰不只是選擇個別技術，而是在需求持續演進時，維持一套能將這些技術與企業資訊、人員、應用、安全及組織營運連結的架構。

Cyberhood 並非由任何單一伺服器、儲存技術、安全機制、協作工具或企業應用所定義，而是由連結它們的架構所定義。

透過分散式基礎架構、共用平台服務、受保護資訊、企業協作、業務應用與可擴充開發框架，Cyberhood 為分散式企業運算建立統一基礎。

基礎架構 → 平台服務 → 企業能力 → 業務營運

身分 → 驗證 → 授權 → 受保護資源

建立 → 儲存 → 分享 → 協作 → 版本化 → 搜尋 → 保護

業務責任各自專業化；平台服務共享。

一個平台架構 — 多種部署模式。

目前需求 → 模組化演進 → 未來能力

最終成果不是固定的科技配置，而是一套設計為能與企業共同演進的架構基礎。

Cyberhood 並非由其所包含的技術來定義，而是由連結這些技術的架構所定義。

Cyberhood

一個分散式平台。一套企業架構。為持續演進而打造。

架構願景中的企業應用整合

Cyberhood 企業應用整合將平台願景從分散式基礎架構與受保護資訊延伸至協調一致的企業營運。平台連接專業化應用，而不消除其專業化責任。

分散式架構提供參與基礎架構的營運基礎；Cyberhood SPAN 為採用 SPAN 保護的資訊提供受保護資訊架構；企業應用整合則連接專業化企業應用之間的 API、交易、訊息、資訊流、工作流程狀態與企業流程。

這些能力形成互補的架構關係，不要求所有應用變得相同、所有服務集中化，或所有資訊位於同一實體位置。架構提供共同關係，使專業化能力能在一致的企業環境中運作。

專業化應用 — 整合流程 — 共享平台服務 — 一個企業架構

平台連接專業化應用，而不消除其專業化責任。

一個分散式平台。一套企業架構。為持續演進而打造。

附錄 A

技術詞彙

本詞彙表定義《Cyberhood 分散式企業平台國際白皮書》中使用的主要架構、平台、資訊保護、應用與部署術語。這些定義用以說明各術語在 Cyberhood 架構中的使用方式；若某術語在業界具有更廣泛的含義，以下定義則說明其在本白皮書中的特定脈絡。

Cyberhood 分散式企業平台

一套分散式企業平台架構，在同一個協調一致的架構環境中，連結分散式基礎架構、共用平台服務、身分與授權、企業安全、受保護資訊、協作與資訊服務、企業應用，以及應用擴充能力。

它代表共同的架構基礎，使專業化的企業能力得以參與分散式企業營運。

分散式基礎架構（Distributed Infrastructure）

由運算、儲存、網路、分散式節點及其他參與的基礎架構資源所構成，為 Cyberhood 平台跨一個或多個部署環境提供技術基礎。

分散式平台服務（Distributed Platform Services）

運作於分散式基礎架構之上的共用平台能力，用以支援更高層級的企業服務與應用。這些能力包括身分驗證、授權、索引、分散式儲存服務、工作流程、訊息傳遞、SDK 服務、管理，以及本白皮書所述的其他參與式平台服務。

Master Node

Cyberhood 分散式架構中的主要節點角色，依適用的架構與部署設計參與平台協調與服務運作。

Slave Node

參與 Cyberhood 平台的分散式節點角色，依其被指派的架構責任與部署需求提供資源或服務。

分散式本地節點（Distributed Local Node, DLN）

部署於組織或分散式地點的 Cyberhood 節點，用以將平台參與延伸至該環境。分散式本地節點可依部署設計參與被指派的服務、處理、儲存或其他平台責任。

分散式本地節點是更廣泛 Cyberhood 平台架構的一部分，而非獨立運作的平台。

Cyberhood SPAN — Secured & Protected Archive Network

Cyberhood 分散式企業平台的受保護資訊架構。SPAN 透過受保護分段、加密、分散式配置、門檻式重建、裝置層級容錯與保護狀態復原，使邏輯企業資訊降低對個別儲存資源的依賴。

SPAN 作為整體 Cyberhood 架構的 Protected Information Layer，並可依平台與部署設計使用參與的儲存資源。

Global Index（全域索引）

Cyberhood 平台的索引能力，依平台存取與授權關係，支援跨參與資訊資源的資訊探索與全文搜尋。

高可用性（High Availability, HA）

一種架構方法，透過參與的分散式資源、故障偵測、隔離、重新分配、復原與容量恢復，支援服務持續性。

高可用性主要著重於在適用的故障條件下持續提供服務，不應被視為與災難復原相同。

災難復原（Disaster Recovery, DR）

一種以復原為導向的架構方法，著重於重大中斷後恢復服務與資訊。

DR 著重服務恢復，高可用性則著重服務持續性；兩者互補，但在架構上彼此不同。

身分驗證（Identity Authentication）

Cyberhood 平台在考慮允許存取適用的平台資源或服務之前，用以驗證參與使用者或應用身分的程序。

授權（Authorization）

平台用以判斷已驗證身分是否被允許存取應用、服務、資訊資源或其他受保護資源，或對其執行適用動作的程序。

Independent Firewall

Cyberhood 安全架構中的主機保護能力，作為更廣泛分層安全模型的一部分，用以保護參與的分散式主機。

企業協作（Enterprise Collaboration）

原生平台能力，連結人員、身分、通訊、企業資訊、分享、搜尋、版本管理、工作空間、應用與組織流程。

在 Cyberhood 架構中，協作連結人員、資訊與工作，而非僅作為孤立的通訊功能。

我的空間（My Space）

Cyberhood 中代表使用者個人資訊環境的邏輯工作空間。

公共空間（Public Space）

Cyberhood 中供較廣泛且經授權之組織成員使用資訊的邏輯工作空間。

我分享的空間（Sharing With Space）

Cyberhood 的邏輯工作空間關係，代表我分享給其他人的資訊。

分享給我的空間（Shared From Space）

Cyberhood 的邏輯工作空間關係，代表其他人分享給我的資訊。

企業應用生態系統與整合

與 Cyberhood 平台共同運作的專業化企業應用集合，包括 Workflow、Project Management、CRM、ERP 及相關組織能力。

應用在參與共同平台架構的同時，仍保有各自專業化的業務責任。

企業應用整合（Enterprise Application Integration）

Cyberhood 已實作的平台能力，透過共享企業流程與整合機制連接多個專業化企業應用，同時保留各應用的專業化業務責任。

企業整合服務（Enterprise Integration Services）

Cyberhood 用以連接參與企業應用與服務的已實作整合能力，包括 API Integration、Transaction Orchestration、Enterprise Service Bus（ESB）、Message Bus 與 Automatic Cross-Application Synchronization。

API Integration

透過已定義的應用介面，使參與應用與服務交換功能能力與資訊的整合能力。

交易編排（Transaction Orchestration）

協調跨越應用邊界之業務活動與交易關係的整合能力。

Enterprise Service Bus（ESB）

使參與服務與應用在 Cyberhood 企業應用環境中進行協調式互動的共享企業整合能力。

Message Bus

支援參與應用與平台元件之間訊息通訊與事件交換的訊息型整合能力。

Automatic Cross-Application Synchronization

依整合式企業流程需求，維持參與應用之間相關資訊與流程狀態關係的已實作能力。

跨應用流程協調（Cross-Application Process Orchestration）

協調跨越多個專業化應用的企業流程。在 Cyberhood 中，工作流程／電子簽核可作為跨應用流程協調能力，連接業務活動、電子簽核、組織授權、電子文件、內部稽核、內部控制與後續應用處理。

Cyberhood SDK

Cyberhood 提供的共同軟體開發基礎，使額外應用可與 Cyberhood 分散式平台服務及參與的平台資源建立關係。

Distributed Application Framework

一套架構框架，使 Cyberhood 應用可依應用設計，與身分驗證、Distributed Service Selection、應用處理、平台資源及分散式基礎架構建立關係並運作。

Distributed Service Selection（分散式服務選擇）

Cyberhood 平台機制，使應用可依平台模型辨識適當的參與服務主機，並在適用時考量距離或效能。

Distributed Service Selection 不應被解讀為通用的自動應用容錯移轉。

私有企業部署（Private Enterprise Deployment）

Cyberhood 主要運作於組織所控制基礎架構上的部署模式。參與的基礎架構可位於一個或多個組織地點。

私有部署不等於單一站點部署。

私有雲部署（Private Cloud Deployment）

Cyberhood 運作於由組織控制或專用的雲端導向基礎架構上，同時維持整體 Cyberhood 平台架構的部署模式。

混合雲部署（Hybrid Cloud Deployment）

依企業需求，使私有基礎架構與外部或雲端導向基礎架構共同參與整體 Cyberhood 平台架構的部署模式。

多站點企業部署（Multi-Site Enterprise Deployment）

總部、分公司、區域設施或其他組織站點共同參與 Cyberhood 平台架構的部署方式。

參與站點不一定需要相同的實體基礎架構或相同的服務配置。

復原導向部署（Recovery-Oriented Deployment）

一種部署架構，用以提供重大中斷後恢復適用服務與資訊所需的資源及架構關係。

復原導向部署與高可用性架構互補，但其本身並不定義通用的復原目標、RPO、RTO 或自動地理容錯移轉。

Protected Information Layer（受保護資訊層）

Cyberhood SPAN 對適用企業資訊提供受保護分段、加密、分散式配置、門檻式重建、裝置層級容錯與保護狀態復原的架構層。

Protected Information Layer 與實體儲存基礎架構相關，但在架構上彼此不同。

受保護資訊（Protected Information）

透過適用的 Cyberhood 授權、安全與資訊保護關係處理的企業資訊。當 SPAN 保護適用時，受保護資訊可參與分段、加密、分散式配置、門檻式重建、已設定容錯及保護狀態復原。

並非每一個應用或每一類資訊都會自動受到 SPAN 保護。

模組化擴充（Modular Expansion）

隨需求演進，透過增加運算資源、儲存資源、分散式節點、組織站點或平台容量來擴充 Cyberhood 的架構能力。

模組化擴充在允許實體資源與部署拓樸演進的同時，維持整體架構模型。增加儲存資源會創造更多架構選項，但不會自動提高 SPAN 的容錯能力。

業務服務（Business Services）

由企業應用與底層 Cyberhood 平台架構所支援的組織活動、營運能力與業務責任。

Cyberhood 架構框架（Cyberhood Architecture Framework, CAF）

描述分散式基礎架構、分散式平台服務、協作與資訊服務、企業應用及業務服務如何在 Cyberhood 分散式企業平台中相互關聯的邏輯架構參考框架。

CAF 亦描述涉及身分、安全、受保護資訊、分散式應用架構與部署架構的跨層關係。CAF 是邏輯架構框架，而非強制性的實體部署拓樸。

附錄 B

參考架構

本附錄提供概念性參考架構，彙整本白皮書所定義的主要架構關係。這些模型說明 Cyberhood 基礎架構、平台服務、資訊、安全、應用與組織環境之間的邏輯關係。它們是參考模型，而非強制性的實體拓樸；實際實作可依企業需求、參與資源、服務配置、資訊配置與部署設計而異。

B.1 Cyberhood 企業平台參考架構

目的 — 說明組織使用者與業務服務如何透過專業化企業應用、協作與資訊服務、共用平台服務及分散式基礎架構運作。

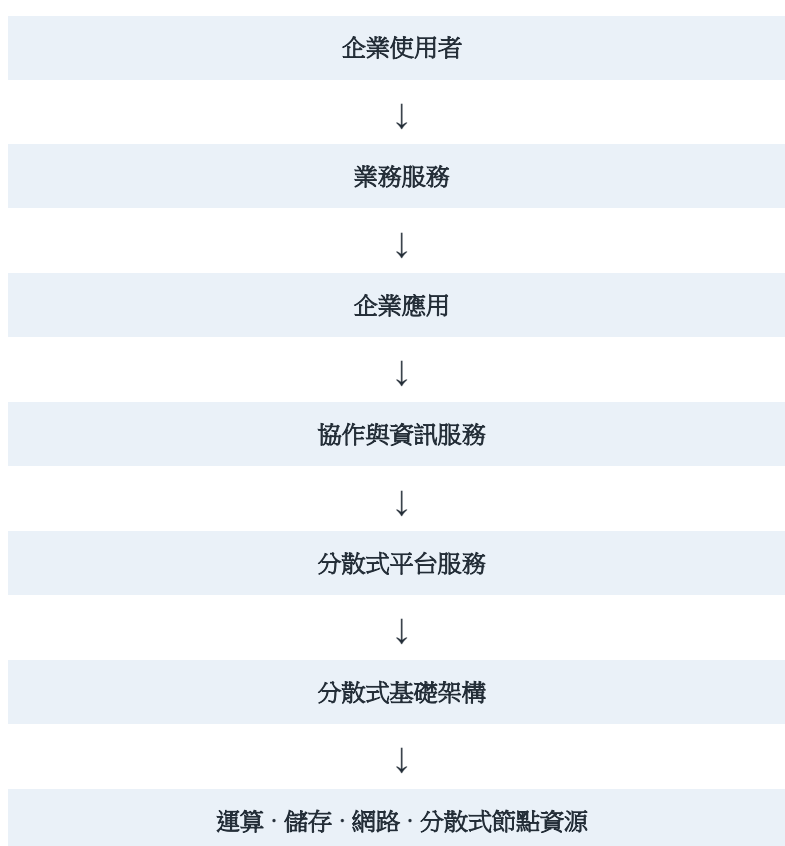


圖 B-1 — Cyberhood 企業平台參考架構

安全、身分與授權，以及受保護資訊，作為彼此相關的跨層責任運作。

關鍵關係 — 業務服務代表平台所支援的組織能力。企業應用保有專業化的業務責任，同時與共用平台能力建立關係。分散式平台服務與分散式基礎架構則為更高層級的企業能力提供共享架構基礎。

業務責任各自專業化；平台服務共享。

架構考量 — 此模型分離架構責任，但不隔離架構參與。安全跨越各層運作，而非獨立的應用層。適用時，受保護資訊可透過 Cyberhood SPAN Protected Information Layer 參與協作與應用。

責任分離不代表架構必須分離。

B.2 企業應用整合參考架構

目的 — 說明專業化企業應用如何透過已實作的企業整合服務參與共享企業流程，同時保留其專業化業務責任。

專業化企業應用 ↔ 共享企業流程與工作流程整合 ↔ 企業整合服務 ↔ Cyberhood 平台核心服務 ↔ Cyberhood SPAN ↔ 分散式基礎架構

企業整合服務包括 API Integration、Transaction Orchestration、Enterprise Service Bus (ESB)、Message Bus 通訊與 Automatic Cross-Application Synchronization。工作流程／電子簽核為電子簽核、電子文件、組織授權、內部稽核、內部控制與後續業務處理提供跨應用流程協調關係。

關鍵關係 — 應用維持專業化；企業流程可跨越應用邊界；整合服務連接 API、交易、訊息、資訊流與流程狀態；共同平台服務由參與應用共享。

應用整合不要求功能趨同。

B.3 分散式基礎架構參考架構

目的 — 說明 Cyberhood 節點角色與基礎架構資源如何參與更廣泛的平台環境。

參與節點角色	分散式資源
Master Nodes	運算
Slave Nodes	儲存
分散式本地節點 (DLN)	網路

圖 B-2 — 分散式基礎架構參考架構

Cyberhood 平台 ↔ 參與節點與資源 ↔ 組織站點／部署環境

關鍵關係 — 節點角色代表架構參與，而非通用硬體配置。分散式本地節點依被指派的服務與部署需求，將 Cyberhood 平台延伸至組織地點。各站點參與的運算、儲存與網路資源可有所不同。

架構考量 — 共同平台架構不要求各站點採用相同架構。多個參與資源可提供韌性的架構基礎，但實際服務持續性取決於服務設定與部署設計。分散式本地節點是整體平台架構的一部分，而非獨立平台。

分散式架構 ≠ 自動高可用性。

B.4 受保護資訊參考架構

目的 — 說明以身分為基礎的存取控制、企業資訊使用與 Cyberhood SPAN Protected Information Layer 之間的關係。

存取控制關係	受保護資訊關係
身分	企業資訊
驗證	Cyberhood SPAN
授權	分段與加密
應用與協作	分散式配置
企業資訊	門檻式重建
	保護狀態復原

圖 B-3 — 受保護資訊參考架構

存取控制與受保護資訊架構彼此相關，但在架構上不同。

關鍵關係 — 身分、驗證與授權治理誰可以存取企業資訊。應用與協作服務決定經授權資訊如何參與組織工作。Cyberhood SPAN 則治理適用的受保護資訊如何被分段、加密、分散、重建與復原。

架構考量 — SPAN 不會自動保護每個應用或資訊類別。地理分散的受保護資訊配置不會自動建立地理服務容錯移轉。增加儲存資源也不會自動提高已設定的容錯能力。

資訊是邏輯企業資源；儲存是基礎架構資源。

B.5 多站點企業參考架構

目的 — 說明地理或組織上分散的地點如何參與共同的 Cyberhood 平台架構。

企業地點	平台參與
總部	分散式本地節點
分公司	參與平台節點
區域設施	Cyberhood 平台服務
分散式站點	分散式基礎架構資源

圖 B-4 — 多站點企業參考架構

共同企業架構不要求各站點具有相同的基礎架構。

關鍵關係 — 組織站點可參與共同平台，而不要求每個地點具備相同基礎架構。服務配置、應用配置與受保護資訊配置可因站點而異。使用者可依身分與授權關係，跨地點參與協作與企業資訊服務。

架構考量 — 多站點架構不會自動代表 Active-Active 區域服務、通用應用複寫或自動地理容錯移轉。地理基礎架構分布、地理服務分布與地理受保護資訊分布彼此相關，但在架構上不同。

使用者位置 ≠ 資訊位置 · 應用位置 ≠ 完整資訊位置

參考架構原則

- 邏輯架構與實體拓樸彼此相關，但在架構上不同。
- 安全跨越整體架構運作，而非獨立的一層。
- 服務配置與受保護資訊配置彼此相關，但不同。
- 分散式架構提供基礎；部署設計決定營運行為。
- 一個平台架構 — 多種部署模式。

附錄 C

技術重點

本附錄提供本白皮書主要 Cyberhood 架構能力的技術摘要，作為技術評估的精簡參考；內容彙整架構特性與關係，而非取代正文中的詳細說明與實作考量。

C.1 分散式架構

- 分散式基礎架構依部署需求納入 Master Nodes、Slave Nodes、分散式本地節點、運算資源、儲存資源、網路資源及參與的組織地點。
- 原生分散式設計 — 分散式資源是平台基礎的一部分，而非中央集中式架構的選配延伸。
- 共同平台架構的設計，使企業服務降低對單一伺服器、儲存裝置或組織地點的依賴。
- 可透過增加節點、儲存資源、參與站點與平台容量進行模組化擴充。
- 分散式架構為韌性與多站點營運提供基礎，但其本身不保證高可用性或自動地理容錯移轉。

C.2 高可用性與韌性

- 高可用性架構透過參與的分散式資源、故障偵測、隔離、重新分配、復原與容量恢復，支援服務持續性。
- 分散式架構中的連線、資料與運算負載平衡概念。
- 高可用性著重服務持續性；復原導向架構著重服務恢復。
- 在適當的服務與資源被設定參與時，分散式部署可降低對個別基礎架構元件的依賴。
- 僅有多個資源並不構成高可用性。實際持續性取決於部署設計、參與服務、資源設定與適用的故障條件。

C.3 安全與資訊保護

- 身分驗證與授權作為基礎存取控制關係：身分 → 驗證 → 授權 → 受保護資源。
- 參與分散式主機的安全通訊機制與 Independent Firewall 保護。
- 在受保護加密儲存之前進行惡意程式掃描。
- Cyberhood SPAN 作為 Protected Information Layer，對適用企業資訊支援受保護分段、加密、分散式配置、門檻式重建、已設定容錯及保護狀態復原。
- 安全跨越架構各層運作，而非獨立的應用層。
- 受保護資訊架構無法消除所有安全風險，且 SPAN 不會自動套用至每個應用或資訊類別。

C.4 協作與資訊服務

- Enterprise Mail 與 Enterprise Messenger 提供組織通訊。
- 檔案管理、版本控制、全文搜尋、分享與跨平台資訊存取。
- 邏輯工作空間模型：我的空間（My Space）・公共空間（Public Space）・我分享的空間（Sharing With Space）・分享給我的空間（Shared From Space）。
- 企業資訊生命週期：建立 → 儲存 → 分享 → 協作 → 版本管理 → 搜尋 → 保護。
- 協作服務在整體平台架構中連結人員、通訊、企業資訊與組織工作。
- 工作空間是邏輯資訊環境，而非實體站點邊界。

C.5 企業應用與整合

企業應用生態系統與整合包括 EIP、工作流程／電子簽核、ERP、CRM、專案管理、通訊與協作，以及其他整合式企業應用。

企業應用整合是已實作的平台能力，連接應用 API、交易、訊息、資訊流與企業流程。

企業整合服務包括 API Integration、Transaction Orchestration、Enterprise Service Bus（ESB）、Message Bus 通訊與 Automatic Cross-Application Synchronization。

工作流程／電子簽核既是專業化應用能力，也是跨應用流程協調機制，連接電子簽核、電子文件、組織授權、內部稽核、內部控制與後續業務處理。

Cyberhood SDK 與分散式應用框架提供開發基礎，使額外應用可依應用設計與平台及整合能力建立關係並運作。

業務責任各自專業化；平台服務共享。應用整合不要求功能趨同。

C.6 部署與擴充

- 架構部署模式包括私有企業、私有雲、混合雲、多站點企業、分散式本地節點與復原導向部署。
- 不依賴特定供應商的概念性混合架構，不受特定公有雲供應商綁定。
- 邏輯平台架構與實體部署拓樸分離。
- 一個平台架構 — 多種部署模式。
- 模組化架構可隨運算容量、儲存資源、分散式節點、組織站點、應用與企業需求持續演進。
- 私有部署 ≠ 單一站點部署。邏輯一致性不要求實體一致。
- 地理基礎架構分布、地理服務分布與地理受保護資訊分布彼此相關，但在架構上不同。

C.7 架構摘要

Cyberhood 技術能力被設計為協調一致的分散式企業架構之一部分，而非彼此孤立的技術領域。

分散式基礎架構 → 共用平台服務 → 安全與受保護資訊 → Enterprise Integration Services → 協作與企業資訊 → 整合式企業應用 → 協調式企業流程 → 業務營運

Cyberhood 的架構價值不僅來自個別能力，更來自連結這些能力的關係。

附錄 D

Cyberhood 架構框架（Cyberhood Architecture Framework, CAF）

D.1 Cyberhood 架構框架的目的

Cyberhood 架構框架（CAF）提供統一的邏輯參考模型，用以理解分散式基礎架構、共用平台服務、企業整合服務、協作、企業資訊、專業化應用、安全與部署架構，如何共同參與協調一致的企業平台。CAF 描述架構責任與關係，而非規定單一強制實作拓樸，因此可應用於不同的組織環境、基礎架構設定、部署模式及企業演進階段。

CAF 定義架構關係 — 而非強制性的實體配置。

此框架描述有哪些責任以及彼此如何關聯；部署設計則決定它們在何處運作。

D.2 CAF 分層架構

CAF 將 Cyberhood 架構組織為邏輯責任層與跨層關係。企業整合服務連接專業化應用、共享企業流程與共同平台能力，同時保留業務責任的區分。

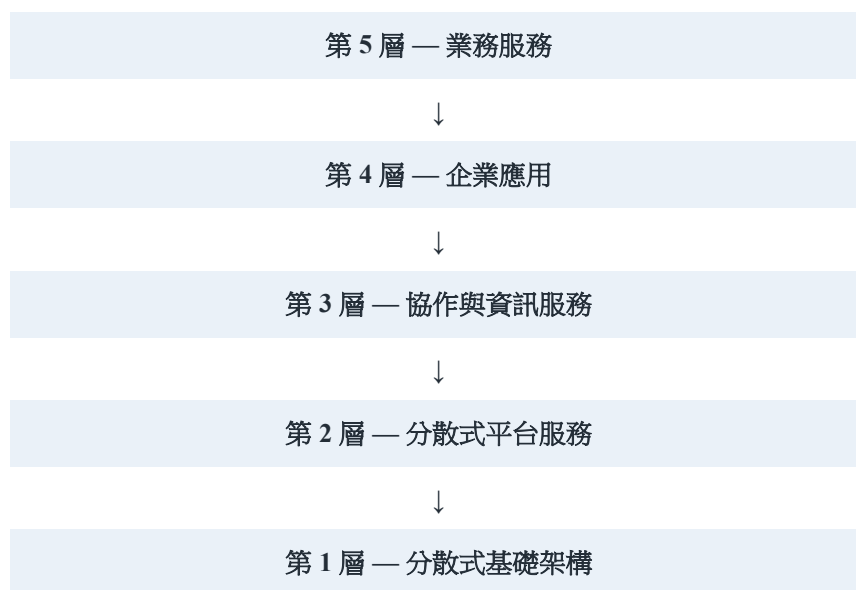


圖 D-1 — Cyberhood 架構框架概觀

跨層責任：身分與授權·安全架構·受保護資訊（Cyberhood SPAN）。部署模式決定參與的實體拓樸。

CAF 各層代表邏輯責任，不一定對應專用的實體系統。

D.3 第 1 層 — 分散式基礎架構

第 1 層提供 CAF 的實體與分散式基礎架構基礎。依部署需求，它包括參與的運算、儲存、網路資源、Master Nodes、Slave Nodes、分散式本地節點及其他基礎架構資源。本層為分散式資源參與、模組化擴充、多站點營運，以及在適當設定下的高可用性設計提供架構基礎。

分散式基礎架構提供韌性的基礎；其本身並不自動構成高可用性。

D.4 第 2 層 — 分散式平台服務

第 2 層提供運作於分散式基礎架構之上的共用平台能力，以支援更高層級的協作、資訊、應用與業務責任。這些能力包括身分驗證、授權、索引、分散式儲存服務、工作流程、訊息傳遞、SDK 服務、管理及本白皮書所述其他共用平台服務。本層的架構目的，是提供不需要由每個業務應用各自重新建立的共享能力。

平台服務是共享的架構能力，而非特定業務責任。

D.5 第 3 層 — 協作與資訊服務

第 3 層將組織使用者與通訊、協作、企業資訊、分享、搜尋、版本管理及邏輯工作空間服務連結。它包括 Enterprise Mail、Enterprise Messenger、檔案管理、我的空間（My Space）、公共空間（Public Space）、我分享的空間（Sharing With Space）、分享給我的空間（Shared From Space）、版本控制、全文搜尋及相關協作能力。本層代表人員、通訊、企業資訊與組織工作之間的架構關係。

通訊連結人員；協作連結人員、資訊與工作。

工作空間是邏輯資訊環境，而非實體站點邊界。

D.6 第 4 層 — 企業應用

第 4 層包含將平台能力轉化為組織流程與業務功能的專業化企業應用，包括 EIP、工作流程／電子簽核、ERP、CRM、專案管理、通訊與協作及相關企業應用能力。應用保有專業化業務責任，同時參與共享的工作流程、整合、資訊與平台關係。

業務責任各自專業化；平台服務共享。

應用參與平台，但不定義平台。

D.7 企業應用整合架構

企業應用整合是平台層級的架構關係，透過共享企業流程與已實作的企業整合服務連接專業化應用。

專業化應用 <-> 共享企業流程與工作流程整合 <-> API Integration / Transaction Orchestration / ESB / Message Bus / Automatic Cross-Application Synchronization <-> Platform Core Services

工作流程／電子簽核提供跨應用流程協調，涵蓋電子簽核、電子文件、組織授權、內部稽核、內部控制與後續業務處理。

平台連接專業化應用，而不消除其專業化責任。

D.8 第 5 層 — 業務服務

第 5 層代表 Cyberhood 架構最終支援的組織活動、營運能力與業務責任。在此層，企業應用、協作、資訊與平台能力共同支援組織流程與業務營運。因此，CAF 將科技架構與企業活動連結，而不把業務責任視為實作意義上的科技層。

D.9 跨層安全架構

在 CAF 中，安全是跨層架構責任，而非獨立的應用層。

身分 → 驗證 → 授權 → 受保護資源

安全機制跨越不同架構責任參與，包括安全通訊、Independent Firewall 主機保護、惡意程式防護、活動紀錄與受保護資訊。不同控制措施依參與的平台服務、應用、資訊資源、基礎架構資源與部署設計而適用。

安全不是單一邊界，而是跨架構層的關係。

安全控制保護元件；安全架構保護關係。

D.10 受保護資訊架構

CAF 將企業資訊視為邏輯企業資產，並使其參與協作、應用、安全與組織流程。

建立 → 儲存 → 分享 → 協作 → 版本管理 → 搜尋 → 保護

Cyberhood SPAN 為適用的企業資訊提供受保護資訊層（Protected Information Layer）。

企業資訊 → Cyberhood SPAN → 分段 → 加密 → 分散式配置 → 門檻式重建 → 保護狀態復原

參與的儲存資源在此邏輯受保護資訊架構之下提供基礎容量。SPAN 不會自動套用至每個應用或資訊類別，且地理分散的受保護資訊配置不會自動建立地理服務容錯移轉。

資訊是邏輯企業資源；儲存是基礎架構資源。

受保護資訊配置與服務配置彼此相關，但在架構上不同。

D.11 分散式應用架構

CAF 定義一種分散式應用關係，使應用可透過 Cyberhood SDK 與 Distributed Application Framework，與共用平台服務及分散式基礎架構建立關係並運作。

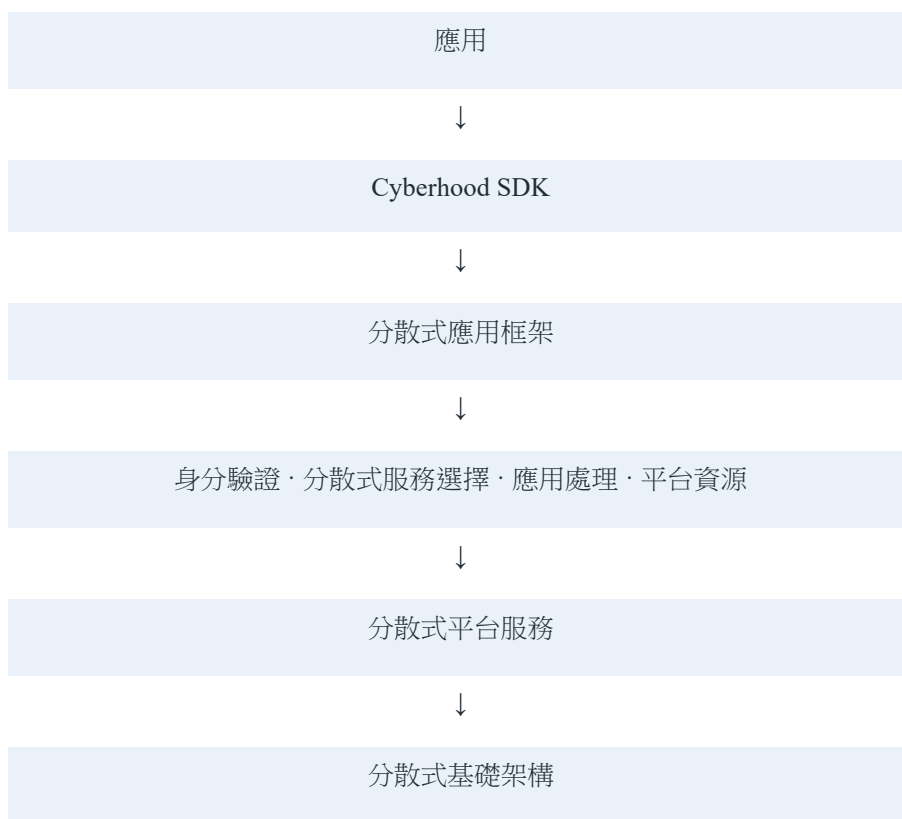


圖 D-2 — 分散式應用架構

應用實際使用哪些平台能力，取決於其設計與需求。

分散式服務選擇（Distributed Service Selection）不代表通用的自動應用容錯移轉。擴充性是平台能力，但不保證每一項未來應用需求都會自動獲得滿足。

D.12 部署架構

CAF 將邏輯平台架構與實體部署拓模分離。



CAF 部署關係

本白皮書所述的支援架構模式包括私有企業、私有雲、混合雲、多站點企業、分散式本地節點與復原導向部署。地理基礎架構分布、服務分布與受保護資訊分布彼此相關，但在架構上不同。

一個平台架構 — 多種部署模式。

邏輯一致性不要求實體一致。

部署改變架構運作的位置 — 而不是架構本質。

D.13 CAF 架構原則

- 原生分散式設計 — 分散式基礎架構是平台基礎的一部分，而非選配延伸。
- 平台優先於產品 — 個別功能與應用參與更廣泛的企業平台架構。
- 身分作為基礎 — 身分連結使用者、組織角色、授權、應用、資訊與企業資源。
- 資訊作為企業資產 — 企業資訊參與儲存、協作、搜尋、應用、安全與組織流程。
- 安全即架構 — 安全跨越架構各層運作，而非單一邊界或獨立層。
- 協作作為原生能力 — 通訊、資訊、分享、工作空間與組織互動共同參與企業平台。
- 業務責任各自專業化；平台服務共享 — 應用保有專業化業務責任，同時參與共用平台能力。
- 一個平台架構 — 多種部署模式 — 不同實體部署環境可套用同一套更廣泛的邏輯平台架構。
- 模組化演進 — 運算、儲存、分散式節點、組織地點與平台容量可隨需求變化而演進。
- 為未來開發提供擴充性 — Cyberhood SDK 與 Distributed Application Framework 為額外應用能力提供架構基礎。

這些原則共同將 CAF 定義為分散式企業運算的邏輯架構框架。CAF 提供共同模型，使基礎架構、平台服務、企業資訊、安全、協作、應用、部署模式與業務責任，可在同一個協調式平台環境中被理解為彼此相關的架構領域。

CAF 定義使專業化企業能力得以在同一套分散式企業架構中運作的關係。

D.14 CAF 架構關係摘要

Cyberhood 架構框架可透過七項主要關係加以概括：

平台關係

分散式基礎架構 → 分散式平台服務 → 協作與資訊服務 → 企業應用 → 業務服務

安全關係

身分 → 驗證 → 授權 → 受保護資源

資訊關係

建立 → 儲存 → 分享 → 協作 → 版本管理 → 搜尋 → 保護

受保護資訊關係

企業資訊 → SPAN → 分段 → 加密 → 分散式配置 → 重建 → 復原

應用關係

應用 → Cyberhood SDK → 分散式應用框架 → 平台服務 → 分散式基礎架構

企業整合關係

專業化應用 ↔ 共享企業流程與工作流程整合 ↔ API Integration / Transaction Orchestration / ESB / Message Bus / Automatic Cross-Application Synchronization ↔ Platform Core Services

部署關係

企業需求 → 部署模式 → 邏輯平台架構 → 分散式基礎架構資源

這些關係構成 CAF 的架構核心。

Cyberhood 架構框架 — 分散式企業營運的一套邏輯架構。

CAF 定義分散式基礎架構、平台服務、企業資訊、安全、協作、應用與部署模式如何在同一套協調式企業架構中參與的架構關係。

Cyberhood 分散式企業平台

架構原則 · 企業價值 · Kinghood Technology

Cyberhood 架構原則

- 原生分散式設計
- 平台優先於產品
- 身分作為基礎
- 資訊作為企業資產
- 安全即架構
- 協作作為原生能力
- 業務責任各自專業化；平台服務共享
- 一個平台架構 — 多種部署模式
- 模組化演進
- 為未來開發提供擴充性

Cyberhood 的企業價值

- 統一架構 — 降低碎片化、複雜度與整合負擔。
- 營運持續性 — 支援服務持續與復原導向營運。
- 資訊保護 — 透過分層安全與 Cyberhood SPAN 保護適用的企業資訊。
- 業務敏捷性 — 隨需求演進調整應用、服務與部署架構。
- 可擴充成長 — 在共同平台架構中擴充使用者、資訊、資源與據點。

Cyberhood

Cyberhood 是一套分散式企業平台架構，連結基礎架構、平台服務、企業資訊、安全、協作、應用與業務營運。其設計旨在支援目前的企業需求，同時提供可隨未來組織與科技需求持續演進的架構基礎。

Kinghood Technology

網站：www.kinghood.com
電子郵件：sales@kinghood.com

Copyright © 2026 Kinghood Technology. All rights reserved.

一個分散式平台。一套企業架構。為持續演進而打造。