Cyberhood®

Cyberhood 分散式企业平台
国际白皮书

简体中文版 | Version 3.4

一个分散式平台。一套企业架构。为持续演进而打造。



分散式
基础架构

资讯保护

企业协作

企业应用

模组化演进

Kinghood Technology

分散式企業解決方案
连结企业、资讯与营运

Version 3.4

www.kinghood.com

© 2028 Kinghood Technology. All rights reserved.

文件资讯

文件	Cyberhood 分散式企业平台 — 国际白皮书（简体中文版）
版本类型	正式出版版
版本	Version 3.4
语言	简体中文
日期	2026 年 9 月
状态	Publication Release
发行者	Kinghood Technology

修订纪录

版本	日期	说明	状态
3.3	2026 年 9 月	繁体中文版正式出版（Traditional Chinese Publication Release）	Publication Release
3.4	2026 年 9 月	企业应用整合架构、第 7 章重构、附录同步与执行摘要强化；以校对后的繁体中文版转制简体中文正式出版版。	Publication Release

如何阅读本白皮书

企业主管可先阅读执行摘要、第 1、2、10 与 11 章。架构师与系统整合商可著重第 2 至 5 章、第 8、9 章及附录 D。系统管理与技术团队则可将平台、安全、储存与部署相关章节作为概念性参考。

适用读者

- CIO 与 CTO
- 企业架构师与解决方案架构师
- IT 管理者与基础架构团队
- 系统整合商与技术合作伙伴
- 开发人员与应用架构师
- 资讯安全与营运专业人员

目录

执行摘要 4

PART I — 愿景 5

企业基础架构挑战 6

Cyberhood 分散式企业平台 7

PART II — 核心技术 12

高可用性（High Availability, HA）架构 13

Cyberhood SPAN：分散式受保护资讯架构 18

企业安全架构 26

PART III — 企业平台 30

企业协作平台 31

企业应用生态系统与整合 35

开发者平台与分散式应用框架 42

PART IV — 架构 48

部署模式与参考架构 49

商业价值与企业优势 61

结论与架构愿景 73

技术词汇 84

参考架构 88

技术重点 91

Cyberhood 架构框架（Cyberhood Architecture Framework, CAF） 93

执行摘要

现代企业需要一个能协调分散式基础架构、保护资讯、整合专业化应用、支援业务持续性与协作，并为持续应用开发提供基础的平台。Cyberhood 以统一的分散式企业架构回应这些需求，而非将能力分散于彼此孤立的产品之中。

Cyberhood 结合三项互补的架构责任。分散式架构提供由 Master Nodes、Slave Nodes 与分散式本地节点（Distributed Local Nodes, DLN）构成的营运基础；Cyberhood SPAN 透过受保护分段、加密、分散配置、门槛重建、装置层级容错与保护状态复原，提供受保护资讯层；企业应用整合则连接专业化应用、交易、讯息、资讯流与企业流程。

在应用层，EIP、ERP、CRM、专案管理、工作流程／电子签核、通讯与协作及其他企业应用，各自保留专业化业务责任，同时参与协调式企业流程。已实作的整合能力包括 API Integration、Transaction Orchestration、Enterprise Service Bus（ESB）、Message Bus、Automatic Cross-Application Synchronization，以及共享的工作流程机制。

Cyberhood SDK 与 Distributed Application Framework 进一步提供共同的开发基础。整体形成一个连接基础架构、受保护资讯、整合服务、专业化应用与协调式企业营运的企业平台，同时保留各业务功能与部署环境应有的责任边界。

平台观点

- 分散式基础架构与高可用性 — 协调分散式资源、负载平衡、故障隔离、重新分配、复原与容量恢复。
- 共同平台服务 — 共享身分、授权、资讯管理、通讯、协作、管理与安全能力。
- 受保护资讯架构 — Cyberhood SPAN 将逻辑企业资讯与个别储存资源的依赖关系分离。
- 企业整合服务 — API Integration、Transaction Orchestration、ESB、Message Bus 与 Automatic Cross-Application Synchronization。
- 企业流程整合 — 工作流程／电子签核协调跨应用流程、组织授权、内部稽核、内部控制与后续处理。
- 专业化应用与扩充能力 — EIP、ERP、CRM、专案管理、协作服务、Cyberhood SDK 与 Distributed Application Framework 共同运作于共享架构中。

One Distributed Platform — 分散式架构、受保护资讯、企业整合、专业化应用与协调式企业营运。

PART I — 愿景

第 1 章

企业基础架构挑战

执行概述

企业 IT 环境必须在可用性、安全性、可扩充性、资讯保护与协作之间取得平衡，同时因应连接分散式使用者与系统日益增加的需求。Cyberhood 平台的定位是整合这些需求，而非仅提供单一软体功能。

独立系统的限制

企业经常分别使用不同产品处理储存、通讯、工作流程、客户管理、企业资源规划与应用开发。彼此分离的系统可能造成重复管理、资讯分散，以及不一致的营运模式。

Cyberhood 所提出的架构方向，是提供一个共同的分散式基础，使多种企业服务能在其上运作。

分散式营运环境

现代企业可能跨越总部、分公司、私有基础架构及不同地理位置营运。分散式架构提供资源协调的模式，同时支援在地部署与集中式管理。

设计目标

- 可用性与韧性
- 可扩充的基础架构成长
- 受保护资讯存取
- 整合式协作
- 企业应用支援
- 可扩充的开发能力

重点摘要

- 企业基础架构日益成为架构层级的问题，而非单一产品可以解决的问题。
- 共同平台可降低不同服务之间的碎片化。
- 分散式设计为多据点营运与未来成长提供基础。

摘要

企业 IT 环境必须在可用性、安全性、可扩充性、资讯保护与协作之间取得平衡，同时因应连接分散式使用者与系统日益增加的需求。Cyberhood 平台的定位是整合这些需求，而非仅提供单一软体功能。

第 2 章

Cyberhood 分散式企业平台

分散式企业运算的统一架构

执行概述

现代企业环境正日益走向分散式运作。使用者、资讯、业务流程、应用程式与基础架构，现今可能分布于总部、分公司、远端据点、行动装置以及与云端连接的环境中。

Cyberhood 以分散式企业平台架构回应此一环境。Cyberhood 并非将储存、通讯、协作、工作流程、安全、企业应用与应用程式开发视为彼此孤立的技术环境，而是提供一个将这些能力连结起来的共同架构基础。

其目标不只是提供更多软体功能，而是建立一个协调一致的平台，使多种企业能力能在一致的架构环境中运作。

2.1 从独立产品走向整合平台

传统企业环境往往随著个别产品的导入而逐步成长。档案管理、讯息传递、工作流程、客户管理、资源规划与应用程式开发，可能各自在不同的基础架构与管理模式上运作。

这可能造成身分管理分散、资讯重复、安全控制不一致、应用整合困难，以及营运复杂度持续增加。因此，架构上的核心问题成为：应由哪些共同基础架构与平台服务来支援整体企业环境？

Cyberhood 从平台观点处理这项挑战。各应用程式仍可服务不同的业务目的，同时运作于共享的架构基础之上。

2.2 Cyberhood 平台概念

Cyberhood 分散式企业平台整合分散式基础架构、负载平衡、身分与授权、资讯保护、分散式储存、协作服务、企业应用、管理，以及应用程式开发。

平台采分层架构组织：分散式基础架构提供底层基础；安全与受保护资讯服务提供保护；平台服务提供共同能力；协作与资讯服务连结人员与组织知识；企业应用支援营运；而业务服务则创造组织价值。

2.3 以分散式基础架构作为基础

Master Nodes、Slave Nodes 与分散式本地节点（Distributed Local Nodes, DLN）在分散式平台中扮演彼此协调的角色。此架构不将所有服务集中于单一巨型环境，而是支援将服务与资源分布于参与的平台基础架构中。

此分散式基础可支援运算服务、连线管理、资料分布、应用程式执行、资讯存取、储存服务及跨地理位置部署。

连线、资料与运算的负载平衡，为工作负载分配与渐进式扩充提供架构基础。

2.4 共同平台服务层

要让多个应用程式在一致的环境中运作，就需要共同服务。Cyberhood 提供共享能力，包括身分验证、授权、资讯索引、工作流程、讯息传递、管理、分散式应用服务及 SDK 整合。

这些服务可在身分管理、存取控制、资讯探索、应用整合、管理及未来扩充等面向提供架构一致性。

2.5 以身分作为平台基础

使用者、应用程式、组织角色与资讯存取权限，都依赖可识别的实体。在 Cyberhood 架构中，身分验证与授权提供存取平台资源的基础服务。

此共同模型可支援档案、共享工作空间、协作服务、企业应用、分散式应用服务及管理功能。

2.6 将资讯视为共享的企业资源

Cyberhood 将档案管理、分享、工作空间组织、版本控制、全文检索及跨平台存取，整合于更广泛的平台架构中。

企业资讯生命周期可理解为：建立 → 储存 → 分享 → 协作 → 版本管理 → 搜寻 → 保护。此流程将协作、资讯探索与保护连结为共同资讯架构的一部分。

2.7 跨层式安全架构

安全机制横跨整体架构，涵盖身分、验证、授权、安全通讯、主机保护、恶意程式侦测及受保护资讯服务。

此模型并非宣称任何单一技术可以消除所有风险；相反地，保护机制分布于身分、通讯、基础架构、资讯与储存等不同层面。

2.8 Cyberhood SPAN 作为受保护资讯层（Protected Information Layer）

Cyberhood SPAN（Secured & Protected Archive Network）是一种分散式加密档案系统架构，设计用于结合资讯保护、分散式储存、容错、复原及可扩充容量。

SPAN 与资讯管理、档案服务、协作、安全、分散式基础架构及灾难复原规划相互连结。因此，它是整体企业资讯架构的一部分，而不是孤立的储存元件。

2.9 建构于共同基础上的企业应用

Cyberhood 平台涵盖 Enterprise Mail、Enterprise Messenger、Workflow、Project Management、CRM、ERP、Calendar 及组织通讯等企业应用领域。

这些应用可与组织身分、授权、资讯服务、工作流程机制、管理、受保护储存及分散式基础架构建立共同的架构关系。

2.10 将协作作为原生平台能力

Cyberhood 透过我的空间（My Space）、公共空间（Public Space）、我分享的空间（Sharing With Space）与分享给我的空间（Shared From Space）等概念，将协作与资讯管理整合。

协作可置于更广泛的架构关系中理解：身分 → 授权 → 工作空间 → 资讯 → 协作 → 保护。

2.11 可延伸的应用程式开发平台

没有任何组织能预先预测所有未来的应用程式、工作流程、整合需求或业务流程。因此，Cyberhood 提供 Distributed Application Framework 与 SDK。

Cyberhood SDK 为使用者互动、应用程式呈现、伺服器端处理、分散式主机选择、验证及平台整合提供基础。这种可延伸性，正是平台架构与固定功能产品集合之间的重要差异。

2.12 平台扩充性与架构演进

随著组织成长、使用者增加、资讯量扩大、新应用导入以及更多据点连线，企业需求也会持续改变。

Cyberhood 架构以模组化扩充为设计原则。随需求演进，可加入额外运算资源、分散式节点、储存容量、地理位置及应用服务。

2.13 Cyberhood 架构模型

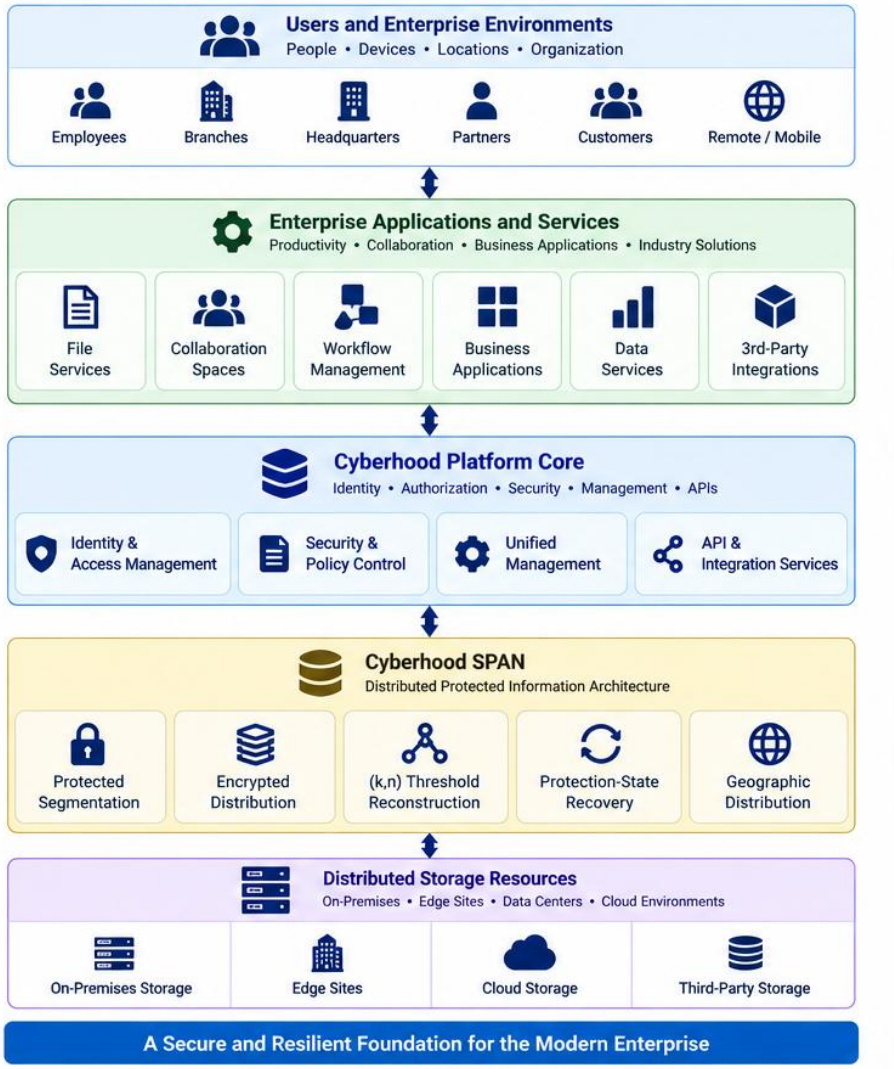


图 2-1　Cyberhood 架构分层模型

基础架构提供底层基础；平台服务提供共同能力；资讯服务连结人员与组织知识；应用程式支援业务营运；Business Services 则创造组织价值。

这项关系构成 Cyberhood 分散式企业平台的核心架构定义。

主要架构原则

Distributed by Design — Cyberhood 以分散式基础架构为设计核心，而非以单一巨型技术环境为基础。

Platform Before Product — 应用程式是更广泛平台架构的一部分，并由共同服务提供支援。

Identity as a Foundation — 身分验证与授权为平台资源存取提供共同控制机制。

Information as an Enterprise Asset — 资讯管理、分享、搜寻、版本管理、协作与保护，在平台架构中彼此连结。

Security by Architecture — 保护机制横跨身分、通讯、基础架构、恶意程式侦测及分散式受保护储存。

Modular Scalability — 基础架构、储存及应用能力可随组织需求演进而扩充。

Collaboration as a Native Capability — 协作直接与企业资讯、身分、存取控制及平台服务连结。

为未来开发提供扩充性 — Cyberhood SDK 与分散式应用框架（Distributed Application Framework）为持续的应用程式开发与整合提供基础。

重点摘要

- Cyberhood 是一个统一的分散式企业平台，而非彼此独立的软体产品集合。
- 此架构连结分散式基础架构、平台服务、安全、资讯管理、协作、企业应用及应用程式开发。
- Master Nodes、Slave Nodes 与分散式本地节点（DLN）提供分散式平台部署的概念基础。
- 连线、资料与运算负载平衡支援可扩充的基础架构运作。
- 共享平台服务为身分、授权、索引、工作流程、讯息传递、管理及应用程式开发提供共同能力。
- Cyberhood SPAN 以分散式加密储存与容错机制为基础，提供受保护资讯层（Protected Information Layer）。
- 企业协作能力将档案、分享、工作空间、版本控制、搜寻、通讯及受保护资讯管理连结起来。
- 企业应用可运作于共同架构基础之上，而不必成为彼此孤立的技术环境。
- Cyberhood SDK 提供扩充平台、加入更多分散式应用程式的途径。
- 此架构透过模组化基础架构与服务扩充，支援长期演进。

摘要

Cyberhood 代表一种企业运算架构方法，透过共同的分散式平台，将基础架构、资讯、安全、协作、应用程式及开发服务彼此连结。

平台从分散式基础架构开始，向上延伸至共享平台服务、受保护资讯管理、企业协作及业务应用。

Cyberhood 不要求每项新服务都建立独立的技术环境，而是提供一个共同平台，让既有与未来的应用程式都能在其上运作。

Cyberhood 并非由任何单一应用程式、储存技术或基础架构元件所定义；其核心价值在于将这些元素连结起来的架构。

Cyberhood 是一个分散式企业平台，旨在于同一个协调一致的架构环境中，整合基础架构、资讯、安全、协作、应用程式及未来创新。

企业应用整合作为平台能力

Cyberhood 将分散式企业平台从基础架构与共同平台服务延伸至整合式企业应用环境。专业化企业应用可参与共享企业流程，同时保留各自业务领域的责任。

平台提供已实作的整合能力，包括 API Integration、Transaction Orchestration、Enterprise Service Bus（ESB）、Message Bus 通讯、Automatic Cross-Application Synchronization，以及共享的工作流程／电子签核机制。这些能力连接企业环境中的应用、交易、讯息、资讯流与组织流程。

此整合层补充而非取代既有平台架构。分散式基础架构提供参与资源；平台核心服务提供共同的身分、授权、资讯、通讯、协作、管理与安全关系；企业整合服务连接专业化应用；Cyberhood SPAN 则在采用 SPAN 保护的资讯范围内提供受保护资讯架构。

分散式基础架构 → 平台核心服务 → 企业整合服务 → 企业应用 → 业务服务

专业化应用 — 共享整合服务 — 一个分散式企业平台

PART II — 核心技术

第 3 章

高可用性（High Availability, HA）架构

为分散式企业环境中的持续运作而设计

执行概述

企业系统即使在个别基础架构元件发生故障时，仍应维持可用。

硬体故障、储存问题、网路中断、软体异常、服务过载及地理区域事件，都是企业运算环境中的现实。因此，高可用性不应仅被理解为部署备援硬体。

具韧性的企业架构必须回答更广泛的问题：当某个元件故障时会发生什么情况？平台如何持续运作，或如何从故障中复原？

Cyberhood 透过分散式架构模型实现高可用性。相较于完全依赖单一集中式伺服器或储存系统，此架构支援将运算、连线、资料与资讯资源分散至多个参与节点。

其目标是降低对个别元件不必要的依赖，并为服务持续性、容错、工作负载分配、基础架构扩充性、复原能力及地理分散部署建立架构基础。

因此，高可用性并非独立功能，而是 Cyberhood 分散式企业平台整体架构的一部分。

3.1 从元件可用性到服务持续性

传统对可用性的讨论通常聚焦于个别元件：伺服器是否正常？储存系统是否可用？网路连线是否正常？应用程式程序是否正在执行？

这些问题固然重要，但不足以完整描述企业可用性。系统中的硬体可能仍正常运作，但关键服务却不可用；反之，个别元件可能发生故障，而整体服务仍可透过其他可用资源持续运作。

因此，Cyberhood 将「元件可用性（Component Availability）」与「服务持续性（Service Continuity）」加以区分。此架构的目标并非防止每一次个别故障。任何基础架构都无法保证所有元件永远持续运作。真正的目标，是降低个别故障对企业所使用服务的影响。

这种以故障为导向的观点，构成 Cyberhood 高可用性模型的基础。

3.2 分散式可用性架构

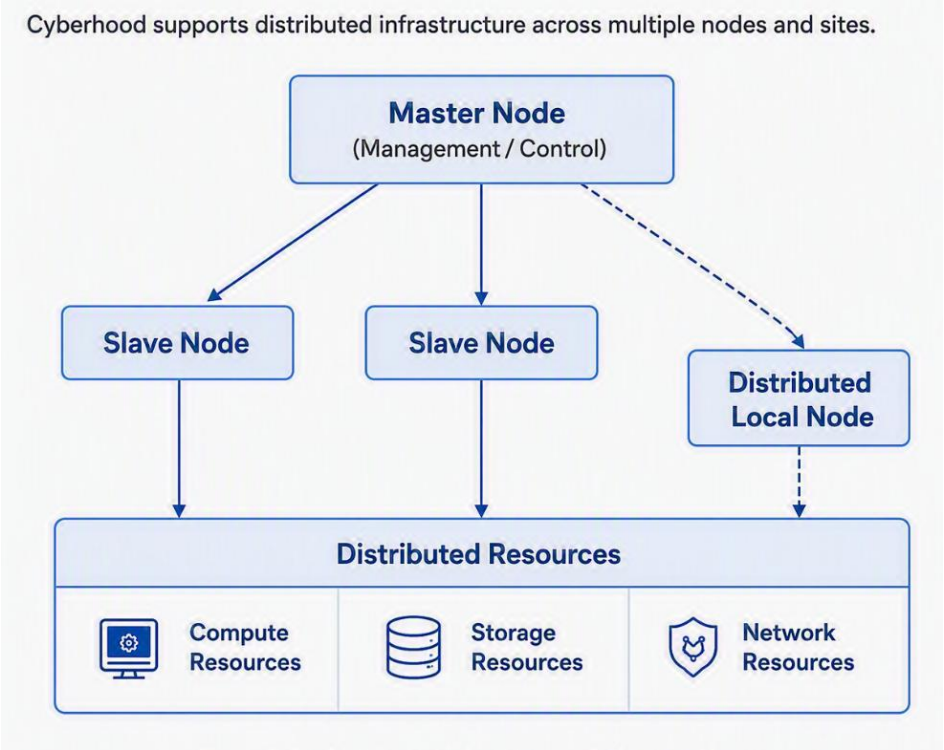


图 3-1 — 分散式基础架构参考模型

Cyberhood 平台以分散式基础架构为核心，包含数种参与节点角色：Master Node、Slave Node，以及分散式本地节点（Distributed Local Node, DLN）。这些角色提供分散平台资源与服务的架构基础。此模型的目的不只是增加伺服器数量，而是建立一个可让服务与工作负载分散于可用基础架构资源之上的环境。

依平台部署与服务设计而定，分散式资源可支援连线处理、应用服务、运算工作负载、资料作业、资讯存取及储存功能。

因此，分散式架构提供了上层高可用性机制得以运作的结构性基础。

3.3 消除不必要的单点依赖

当某一个元件的失效会导致整项服务中断时，即形成单点故障。

分散式架构透过提供替代资源，降低此类依赖；前提是服务设计支援工作负载分配或复原。此原则可应用于运算资源、应用服务、网路连线、储存资源及不同地理位置。

因此，降低不必要的单点依赖，是高可用性的基本原则。

3.4 故障侦测与资源隔离

高可用性要求平台能辨识参与资源何时不再依预期运作。故障侦测之所以重要，是因为当有替代资源可用时，异常资源不应继续接收工作负载。资源隔离则可避免故障或不健康的元件对平台其他部分造成不必要的影响。资源被隔离后，架构可依服务设计及可用基础架构支援选择替代资源。

这形成从「辨识故障」到「控制故障影响」，最终达到「服务持续性」的转换路径。

3.5 连线负载平衡

连线可用性是分散式企业平台的重要面向之一。当使用者或应用程式连接服务时，只要有分散式资源可用，架构就应避免将所有连线活动集中于单一基础架构元件。

Cyberhood 在其分散式架构中纳入连线负载平衡概念。连线分配可降低连线工作负载的集中程度、改善参与资源的利用率、提高基础架构扩充弹性，并降低对单一连线处理资源的依赖。

若某个参与资源变得不可用，连线管理可依部署架构支援使用其余可用资源。

3.6 资料负载平衡

企业平台也必须管理资讯与资料处理工作负载的分配。随著使用者、应用程式与资讯资源增加，集中式系统的需求也会提高。

因此，Cyberhood 将资料负载平衡概念纳入其分散式架构。其目标是提供分配资料相关工作负载的架构基础，而不是将所有处理集中于单一资源。

此模型可支援扩充性、工作负载分配、资源利用及基础架构扩充，同时与 Cyberhood SPAN 等受保护资讯服务建立架构关系。

3.7 运算负载平衡

应用程式的处理需求并非固定不变。更多使用者、更多应用程式、更高交易量、更多资讯处理及扩大的业务营运，都可能增加运算需求。

Cyberhood 纳入运算负载平衡概念，使工作负载可分配至可用的运算资源。这带来两项重要架构效益：工作负载可分散而非集中；当容量需求增加时，也可视需要加入额外运算资源。

因此，分散式架构不仅可在故障情况下提升营运弹性，也能在需求增加期间提供更大的调度空间。

3.8 故障情境模型

情境 1 — 个别节点故障

当个别参与节点变得不可用时，架构目标是避免该故障不必要地影响整体服务。依应用程式的部署模型，可用资源仍可持续提供服务。

情境 2 — 运算资源故障

运算资源可能发生硬体异常、作业系统故障、应用程式程序失效或资源耗尽。在应用程式支援工作负载重新分配的情况下，分散式运算架构可提供替代处理资源，以降低单一运算故障对整体平台的影响。

情境 3 — 储存资源故障

储存故障可能造成重大影响，因为企业服务仰赖资讯的可用性与完整性。Cyberhood 透过受保护资讯架构与 Cyberhood SPAN 处理此关系。分散式加密储存模型旨在为受保护资讯提供容错与复原机制。

情境 4 — 网路或连线故障

网路中断可能使使用者、服务或基础架构资源彼此隔离。分散式部署提供让服务跨多个参与位置或网路路径运作的架构可能性；实际行为则取决于部署架构、网路设计及应用程式设定。

情境 5 — 服务故障

即使底层硬体仍正常运作，服务本身仍可能不可用。因此，服务层级的监控与复原是可用性架构中的重要概念。架构目标是侦测服务故障、在适当情况下隔离异常资源，并利用可用资源恢复服务。

情境 6 — 地理区域或站点故障

局部事件可能影响整个基础架构位置，包括电力中断、网路故障、设施事件、天然灾害或长时间基础架构中断。地理分散式架构可降低单一地点事件自动导致所有平台资源同时丧失的风险，进一步增加韧性。

3.9 高可用性与 Cyberhood SPAN

基础架构可用性与资讯可用性密切相关。如果服务所需资讯无法存取或复原，即使应用服务本身持续运作，也无法提供有意义的持续性。

因此，Cyberhood SPAN 是整体可用性架构的重要组成。SPAN 以分散式储存、加密、容错、复原及容量扩充为基础，提供受保护资讯模型。

因此，高可用性不仅是让应用程式程序维持运作，也包括维持或恢复企业服务所需资讯之存取能力。

3.10 地理分散与灾难复原（Disaster Recovery, DR）

高可用性与灾难复原彼此相关，但处理的是不同的营运目标。

高可用性主要著重于在营运故障期间维持服务持续性；灾难复原则著重于重大中断后恢复服务与资讯。

Cyberhood 分散式架构透过分散式基础架构与受保护资讯服务，提供可同时支援这两项目标的基础。

3.11 将扩充性视为可用性能力

可用性经常只从故障角度讨论，但容量不足同样可能降低服务可用性。服务即使技术上仍在运作，若因过载而无法使用，对使用者而言仍等同于不可用。

Cyberhood 支援透过增加运算资源、分散式节点、储存容量、平台服务及地理位置进行模组化扩充。这使企业能在容量限制演变成服务中断之前，因应成长需求。

3.12 营运持续性模型

完整的 Cyberhood 高可用性模型可概括为持续循环：监控 → 侦测 → 隔离 → 重新分配 → 持续服务 → 复原 → 恢复容量 → 监控。

故障不被视为架构之外的例外事件；相反地，此架构预期基础架构元件可能故障，因此平台必须提供持续运作、复原及恢复能力的相关机制。

关键架构原则

故障导向设计 — 架构会考量基础架构元件变得不可用时应如何处理。

分散式资源 — 运算、连线、资料与资讯服务可分散于参与的基础架构资源。

降低依赖 — 在服务设计支援替代资源的前提下，架构致力降低对个别元件不必要的依赖。

工作负载分配 — 连线、资料与运算负载平衡概念，提供分散营运需求的基础。

故障控制 — 应隔离故障或异常资源，以降低其对整体服务环境造成不必要的影响。

服务持续性 — 目标是维持或恢复企业服务，而非只关注个别元件是否仍在运作。

受保护资讯 — Cyberhood SPAN 将高可用性与受保护资讯、分散式储存、容错及复原连结起来。

地理韧性 — 分散式部署可支援因应局部基础架构或站点层级事件的韧性。

模组化扩充 — 可随组织需求演进加入额外基础架构资源。

重点摘要

- 高可用性是一种维持服务持续性的架构方法，而不只是部署备援硬体。
- Cyberhood 采用包含 Master Node、Slave Node 与分散式本地节点（DLN）的分散式基础架构模型。
- 连线、资料与运算工作负载可分配至参与资源。
- 此架构致力降低不必要的单点依赖。
- 故障侦测与资源隔离提供控制基础架构问题影响范围的概念性路径。
- 依部署与服务架构，可利用其他可用资源支援工作负载重新分配。
- 高可用性除了应用程式与基础架构可用性之外，也必须涵盖资讯可用性。
- Cyberhood SPAN 提供受保护的分散式资讯层，有助于容错与复原。
- 地理分散可增加对局部基础架构或站点层级事件的韧性。
- 扩充性可随营运需求增加而扩大基础架构容量，进而支援可用性。
- 灾难复原与高可用性处理不同目标，但可在共同的分散式架构中运作。

摘要

Cyberhood 高可用性架构建立在一项原则上：企业服务不应不必要地依赖单一基础架构元件持续运作。

透过分散式基础架构、工作负载分配、资源隔离、受保护资讯服务及模组化扩充，此架构为提升服务持续性与复原能力建立基础。

架构目标并不是宣称可以消除故障。故障是企业运算环境中可预期的现实；真正的目标，是让平台能侦测、控制并处理个别故障，而不使其自动演变成整个服务环境的丧失。

因此，Cyberhood 将高可用性视为持续的架构循环：监控 → 侦测 → 隔离 → 重新分配 → 持续运作 → 复原 → 恢复。

此模型将基础架构韧性与资讯保护、扩充性、地理分散及长期营运持续性连结起来。

第 4 章

Cyberhood SPAN：分散式受保护资讯架构

执行概述

企业资讯保护通常结合储存备援、备份、加密、存取控制、恶意程式防护与灾难复原。每一种机制分别处理资讯可用性、机密性、完整性或可复原性的不同面向。

Cyberhood SPAN（Secured & Protected Archive Network）为受保护企业资讯导入分散式方法。SPAN 会将受保护资讯进行分段、加密、分散、储存、重建与复原。其保护模型源自 (k,n) 门槛式秘密分享机制（threshold secret sharing scheme）的原理：受保护资讯会被转换为多个分散式区段，而重建需要达到定义的最少有效区段数量，并具备所需的密码学资讯。

分段 · 加密 · 分散 · 容错 · 重建 · 复原

在 Cyberhood 分散式企业平台中，SPAN 作为 Protected Information Layer 运作。其架构目的，是降低逻辑企业资讯对任何单一实体储存资源的依赖。

4.1 SPAN 架构概述

Cyberhood SPAN 将逻辑企业资讯与用于保护及储存该资讯的个别实体资源分离。在逻辑层级，使用者与企业服务操作的是档案与资讯资源；在保护层级，SPAN 将受保护资讯转换为加密的分散式区段；在实体层级，参与的储存资源提供承载这些受保护区段的基础架构。

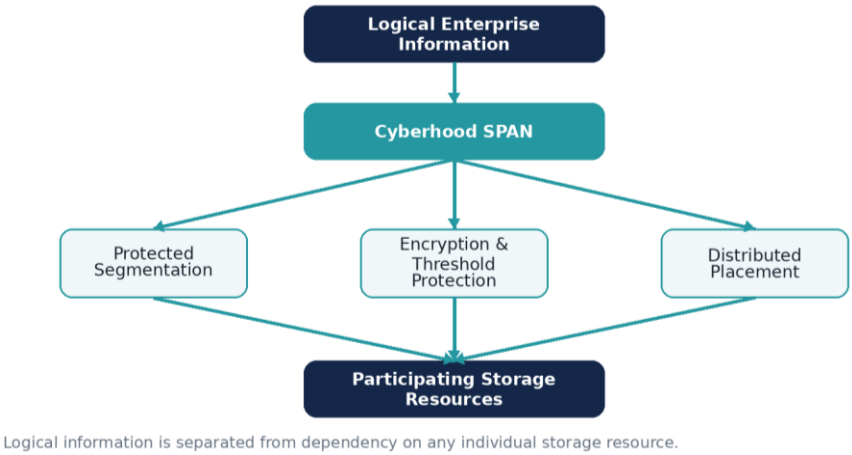


图 4-1 — Cyberhood SPAN 受保护资讯层（Protected Information Layer）

逻辑资讯与对单一实体储存资源的依赖相互分离。

4.2 超越传统备份架构

传统备份架构通常透过保存额外的完整副本来保护资讯。广为采用的 3-2-1 备份原则提供了实用的概念参考：保留多份资讯副本、使用一种以上的储存媒体，并维持地理分离的保护。

SPAN 导入另一种架构模型。受保护资讯不必完全依赖完整副本复制，而可转换为加密区段并分散至参与的储存资源。

备份、高可用性、灾难复原与 SPAN 处理不同的架构责任，彼此可以并存。SPAN 的主要差异在于「分散式受保护资讯重建」，而非只依赖完整副本复制。

4.3 分散式档案分段

SPAN 的第一项核心保护作业，是将逻辑企业档案转换为多个受保护区段。受保护区段的总数以 n 表示，SPAN 再将这些区段分散至参与的储存资源。

因此，一个受 SPAN 保护的档案，是由一组分散式受保护元件所表示，而不是依赖单一储存资源中的完整可用档案。

单一受保护区段并不是完整的原始档案。

4.4 (k,n) 门槛式保护模型

Cyberhood SPAN 采用源自 (k,n) 门槛式秘密分享机制原理的保护模型。在此模型中，n 为受保护区段总数，k 为重建所需的最少有效受保护区段数，且 $k \le n$。

设定的容错关系为 $f = n - k$，其中 f 代表在仍可满足最低重建门槛的情况下，允许不可用的受保护区段数量。例如，若 $n = 7$、$k = 4$，则 $f = 3$。在此示例设定中，重建需要 4 个有效受保护区段；最多可有 3 个区段不可用，而剩余区段数仍不低于重建门槛。

参数	意义	架构角色
n	受保护区段总数	分散式保护集合
k	重建所需的最少有效区段数	重建门槛
$f = n - k$	设定关系可容忍的不可用区段数	容错条件
受保护区段	加密后的分散式元件	将受保护资讯与个别储存资源的依赖分离
参与储存资源	保存受保护元件的资源	分散式保护的实体基础

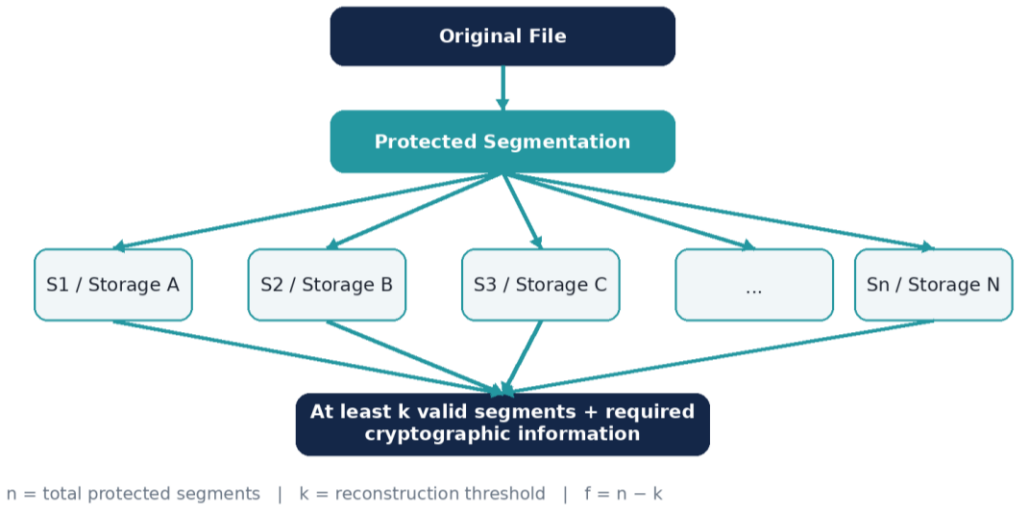


图 4-2 — (k,n) 门槛式分散保护模型

适当的 k 与 n 值应依保护需求及部署设定决定，而不是采用单一通用常数。

4.5 分散式加密与密码学关系

仅有分段并不构成完整的 SPAN 保护模型。SPAN 将受保护分段与加密，以及重建所需的密码学资讯结合。因此，授权重建取决于所需的受保护区段、必要的密码学资讯，以及授权存取。

单一参与储存资源本身，并不预期包含重建完整原始资讯所需的全部条件。

分段 → 加密 → 分散 → 授权 → 重建

4.6 装置层级容错

传统磁碟备援通常保护单一储存设备内的个别磁碟故障。SPAN 则透过将受保护资讯分散于多个参与储存资源，把保护边界延伸至单一储存设备之外。这使单一储存设备内的「磁碟层级备援」与跨分散式储存资源的「装置层级容错」形成明确区别。

因此，参与的储存装置可成为 SPAN 保护架构中的容错单位。

当某个参与资源不可用时，只要可用有效区段数量仍大于或等于 k，受保护资讯仍可重建。底层磁碟备援可与 SPAN 的装置层级保护并存。

4.7 动态容错设定

SPAN 的保护条件可随参与资源环境改变而演进。扩充可用储存资源，可增加受保护区段分配与容错设定的选择；因此，n、k 与 f 之间的关系可依可用环境及保护需求调整。

增加容量并不会自动提高容错能力。实际保护条件取决于可用资源、分散设定、重建门槛及保护政策。

基础架构扩充提供更多保护选项；实际容错条件由保护政策决定。

4.8 装置隔离与 Hot-Swap 作业

只要剩余的保护状态仍符合设定的重建门槛，SPAN 支援隔离异常的参与储存资源，并在整体受保护资讯环境持续运作的情况下加入替代或额外资源。

在此架构中，Hot Swap 指的是在不刻意让整个逻辑受保护资讯环境离线的情况下，隔离、替换或加入参与储存资源的营运能力；它并不代表特定硬体汇流排层级的热插拔实作。

侦测 → 隔离 → 持续运作 → 替换／新增 → 恢复保护

4.9 保护状态复原（Protection-State Recovery）

容错处理的是资源不可用期间如何持续运作；保护状态复原处理的则是之后如何恢复。当不可用资源被隔离或替换后，SPAN 可重新分配受保护资讯，并恢复适当的分散式保护状态。

因此，SPAN 的复原著重于恢复分散式保护关系，而不只是从另一份备份副本还原单一档案。

复原的是保护状态，而不只是单一档案。

4.10 自动化储存分配与平衡

随著资讯成长，以及资源新增、移除、替换或扩充，参与的储存容量会持续变化。SPAN 纳入自动化储存分配与平衡，使受保护资讯能分散于可用的参与资源。

当资源环境改变时，可重新分配受保护资讯，使新增容量参与更广泛的 SPAN 环境，并重新平衡储存利用率。因此，储存平衡同时支援容量利用与保护状态管理。

4.11 加密前的恶意程式防护

Cyberhood SPAN 在受保护分段、加密与分散式储存之前整合 ClamAV 恶意程式检查。于受保护储存前进行扫描，可在逻辑档案被转换为加密分散式元件之前完成恶意程式检查。这可降低受感染内容被保存为受保护企业资讯，之后又被重建并散布至其他端点的风险。恶意程式检查仍只是 Cyberhood 企业安全架构的一部分，不能取代端点安全、身分保护、授权、应用程式安全、网路防护或安全监控。

先检查，再保护（Inspect Before Protect）。

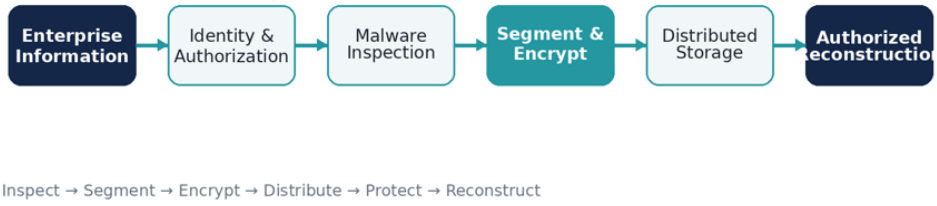


图 4-3 — SPAN 资讯保护流程

4.12 防范装置损坏与资讯遗失

实体储存资源仍可能遭遇硬体故障、断电、实体损坏、环境事件、网路断线或管理性隔离。SPAN 透过分散式分段与门槛式重建，降低受保护资讯对单一资源的依赖。

只要设定的重建门槛仍能满足，即使个别参与资源不可用，受保护资讯仍可保持可重建。SPAN 并不消除实体储存故障，而是降低受保护资讯对任何单一故障事件的依赖。

装置故障 ≠ 自动等同资讯遗失

4.13 防范单一装置遭入侵

分散式受保护资讯会改变单一储存资源遭入侵时的安全影响。由于 SPAN 资讯经过分段、加密与分散，仅取得一个参与储存资源本身，并不足以取得完整原始档案。这可降低资讯机密性对任何单一参与储存资源的依赖。但这不代表端点、授权帐号、应用程式、管理环境或足够数量的参与资源遭入侵时，不会影响资讯安全。

单一储存资源遭入侵，不应等同于完整受保护档案遭入侵。

4.14 具勒索软体韧性的资讯架构

对勒索软体的韧性需要多层安全机制。SPAN 透过分散式受保护分段、加密储存、门槛式重建、装置层级分散、授权关系及保护状态复原，对此韧性提供支援。

此架构可降低单一参与储存资源遭入侵、损坏、加密或变得不可用时的影响。SPAN 并不代表具备全面的勒索软体免疫能力；端点遭入侵、凭证窃取、应用程式弱点、管理环境遭入侵、经授权的破坏性操作及其他攻击途径，仍属整体企业安全架构必须处理的责任。

SPAN 强化勒索软体韧性；但不取代多层企业安全。

4.15 地理分散资讯保护

SPAN 可将受保护资讯元件分散至位于不同网路或地理环境中的参与资源。透过企业网路或 Internet 的点对点通讯，可使受保护资讯的保护边界延伸至单一实体站点之外。

地理分散可降低所有受保护元件对单一实体位置的依赖。应用程式容错移转、Active-Active 服务运作、复原顺序、RPO 与 RTO，则取决于更广泛的部署与复原架构。

地理分散资讯 ≠ 自动地理服务容错移转

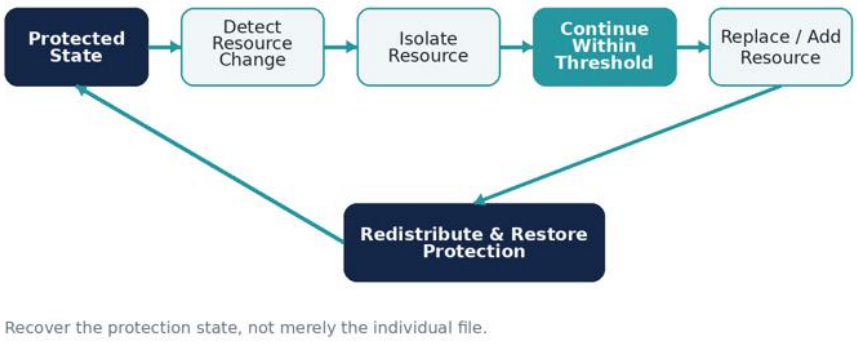


图 4-4 — SPAN 容错与保护状态复原模型

4.16 模组化储存扩充

SPAN 支援透过加入参与储存资源进行模组化储存扩充。新增加的容量可纳入分散式环境，并可随资源设定演进重新分配受保护资讯。传统 NAS 资源也可在更广泛的 SPAN 架构中提供储存容量。

实际可扩充规模仍受基础架构、网路、软体、管理、效能及部署条件限制。其架构价值在于模组化成长。

增加资源 → 扩充容量 → 重新评估分配 → 重新平衡保护

4.17 平行资讯存取与串流

重建所需的受保护元件可能位于多个参与资源。因此，SPAN 可在资讯存取过程中支援从分散式储存资源并行撷取，以及档案串流传送。

平行处理并不代表固定的效能倍增。实际效能取决于网路频宽与延迟、储存效能、档案特性、设定的 k 与 n 关系、同时工作负载、重建处理及部署拓扑。

SPAN 为平行受保护资讯撷取与串流提供分散式基础；实际效能取决于部署条件。

4.18 SPAN 与企业资讯服务

SPAN 位于较上层的 Cyberhood 资讯与协作服务之下，作为受保护资讯基础。使用者与应用程式操作的是逻辑企业资讯，而不是直接管理分散在实体储存资源中的个别受保护区段。

Cyberhood 资讯空间透过平台服务与授权，以逻辑资讯环境呈现，而不是直接存取底层个别受保护区段。

逻辑资讯 ≠ 实体储存位置

企业服务操作资讯；SPAN 管理该资讯的分散式保护。

SPAN 不应被理解为会自动保护每一个 Cyberhood 应用程式产生的所有资料物件。是否使用 SPAN，取决于应用程式设计、平台设定、资讯分类及组织需求。

4.19 SPAN 资讯保护生命周期

SPAN 是受保护资讯的生命周期，而不只是储存目的地。此生命周期由两条互补的营运路径构成。

资讯保护路径

企业资讯 → 身分与授权 → 恶意程式检查 → 受保护分段 → 加密 → 分散配置 → 受保护储存 → 授权撷取 → 门槛式重建 → 企业资讯

保护状态维护路径

受保护状态 → 监控资源环境 → 资源变更／故障 → 辨识与隔离 → 评估剩余保护状态 → 在可用容错条件内持续运作 → 替换／新增资源 → 重新分配受保护区段 → 重新平衡 → 恢复保护条件

第一条路径保护资讯；第二条路径维持保护状态。两者共同形成：保护资讯 → 维持保护 → 重建资讯。

资讯保护是一个生命周期，而不是一次储存事件。

4.20 Cyberhood SPAN 架构模型

完整的 SPAN 架构透过 Protected Information Layer，将逻辑企业资讯与分散式实体基础架构连结起来。

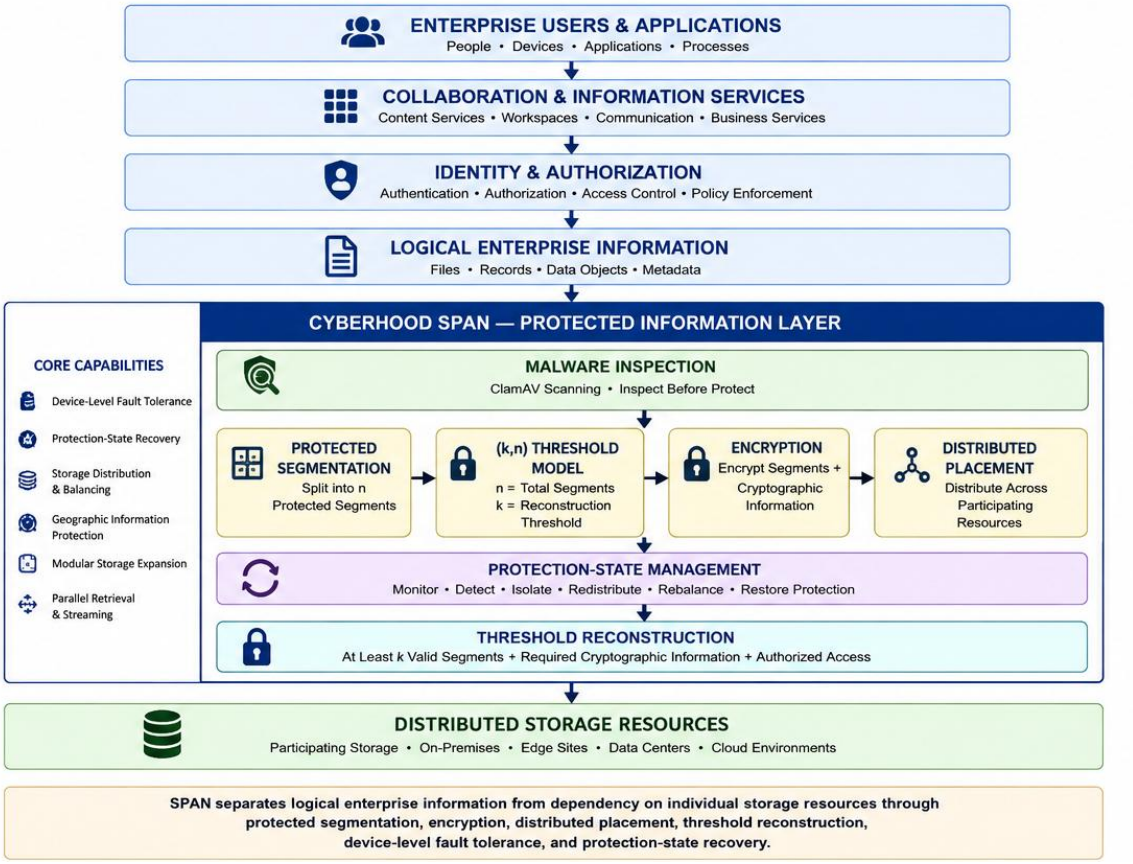


图 4-5 — Cyberhood SPAN 架构模型

因此，SPAN 不只是加密储存。其架构结合分段、加密、分散配置、门槛式重建、装置层级容错、保护状态复原、资源重新分配及资讯生命周期管理。

检查 → 分段 → 加密 → 分散 → 保护 → 监控 → 复原 → 重建

Cyberhood SPAN 是一种分散式受保护资讯架构，透过受保护分段、加密、分散配置、门槛式重建、装置层级容错及保护状态复原，将逻辑企业资讯与对个别储存资源的依赖分离。

Cyberhood SPAN — Cyberhood 分散式企业平台的受保护资讯层（Protected Information Layer）

关键架构原则

- 资讯以分散式关系受到保护 — 保护建立在受保护元件与参与资源之间，而不是只依赖单一完整实体副本。
- 逻辑资讯与实体储存分离 — 企业服务操作逻辑资讯，而 SPAN 管理其分散式受保护表示形式。
- 门槛式重建定义可复原性 — k 与 n 的关系决定重建门槛及设定的容错条件。
- 容错超越个别磁碟 — SPAN 将保护延伸至跨分散式储存资源的装置层级容错。
- 个别资源故障不会自动等同资讯遗失 — 只要仍有足够的有效受保护区段，资讯即可维持可重建。
- 保护状态必须可复原 — 复原包括恢复分散式保护关系，而不只是撷取单一档案。
- 先检查，再保护 — 恶意程式检查先于加密分散式储存。
- 地理分散延伸保护边界 — 受保护元件可跨不同位置参与，而不代表自动服务容错移转。
- 储存成长延伸保护架构 — 增加参与资源可扩充容量，而不改变 SPAN 的基本模型。
- 资讯保护是一个生命周期 — 保护持续涵盖储存、监控、资源变更、重建、重新分配及保护状态复原。

重点摘要

Cyberhood SPAN 建立在五项核心资讯保护概念之上：分段 · 加密 · 分散 · 容错 · 重建。

分段 → 加密 → 分散 → 容错 → 重建

监控 → 侦测 → 隔离 → 重新分配 → 恢复保护

这些能力共同建立 SPAN 作为 Cyberhood 分散式企业平台的 Protected Information Layer。其差异不只是资讯经过加密或储存在多个装置，而是逻辑企业资讯透过分散式关系受到保护，从而降低对任何单一储存资源的依赖。

摘要

企业资讯保护通常结合储存备援、备份、加密、恶意程式防护、存取控制、高可用性及灾难复原。Cyberhood SPAN 处理的是一项不同的架构责任。

SPAN 不让受保护企业资讯完全依赖储存在个别实体储存资源中的完整档案，而是将其转换为分散、加密且可依门槛重建的关系。逻辑企业档案可被分段并分散至参与储存资源，而设定的 (k,n) 关系决定重建所需的最少有效受保护区段数，以及相对应的容错条件。

单一储存装置并不等于资讯本身

单一受保护区段并不是完整档案

单一装置故障不会自动等同资讯遗失

SPAN 进一步透过装置层级容错、资源隔离、保护状态复原、自动化储存分配、恶意程式检查、地理分散资讯保护、模组化扩充及分散式撷取延伸此基础。这些能力是对企业安全、高可用性、备份及灾难复原架构的补充，而不是取代。

SPAN 保护的是企业资讯与其所依赖分散式基础架构之间的关系。

企业资讯不应只依其储存位置受到保护，也应透过如何分段、加密、分散、授权、重建及复原来获得保护。

第 5 章

企业安全架构

执行概述

安全是一项横跨身分、授权、安全通讯、Independent Firewall 防护、恶意程式防护与受保护资讯储存的架构能力。Cyberhood 将这些机制整合于整个分散式企业平台，而非将安全视为独立附加功能。

5.1 安全作为架构原则

企业安全必须保护资讯、通讯、基础架构、身分，以及对组织资源的存取。Cyberhood 将资讯安全视为整合于分散式平台中的架构能力。

Cyberhood 安全架构结合：

- 安全通讯 + 分散式基础架构防护 + 系统化资讯保护

这些能力与身分及授权机制共同运作，建立多层式企业安全环境。

5.2 安全网路通讯

通讯安全是分散式企业平台的基本需求。Cyberhood 采用 SSL 等级或更高等级的安全通讯协定，并结合平台加密机制，以保护传输中的资讯。

5.3 分散式主机防护

分散式平台包含多个基础架构节点，因此仅保护网路周界并不足够。

Cyberhood 为分散式主机提供 Independent Firewall，建立额外的防护边界，以降低未经授权存取企业资讯与资产的风险。

5.4 系统化资讯保护

企业资讯在整个生命周期中都需要受到保护。Cyberhood 将系统化资料保护与个人化授权结合，建立组织身分、使用者帐号、组织角色、资源权限与资讯存取之间的关系。

5.5 组织身分与帐号管理

Cyberhood 将组织帐号管理纳入企业协作环境。个人帐号是资源权限管理的基础，并可依组织需求对应一个或多个组织角色。

5.6 身分验证与授权

身分验证用以确认谁正在要求存取；授权则决定已通过验证的身分可存取哪些资源。Cyberhood 将个人帐号与资源权限及组织角色连结，以建立对企业资讯的受控存取。

5.7 个人化授权

企业组织具有不同的职责、部门、专案与组织角色。Cyberhood 支援个人化授权，使资讯存取能对应组织角色与使用者帐号。

5.8 横跨企业资讯服务的安全

安全控制不仅限于档案储存。Cyberhood 将资讯保护整合至 Enterprise Mail、Enterprise Messenger、档案管理、Workflow、Project Management、CRM、ERP 及相关企业服务与应用。

因此，只要企业服务处理或交换资讯，安全机制就应随资讯而存在。

5.9 档案存取保护

Cyberhood 的档案管理环境提供我的空间（My Space）、公共空间（Public Space）、我分享的空间（Sharing With Space）与分享给我的空间（Shared From Space）等不同资讯空间。这些空间结合帐号权限与授权，形成控制资讯存取的结构化模型。

5.10 分散式资讯保护

Cyberhood SPAN 将安全架构延伸至受保护储存。SPAN 是分散式加密档案系统，结合资讯保护、分散式储存、容错、复原与可扩充容量。

存取控制决定谁可以存取资讯；加密保护分散式储存架构中的资讯；分散配置与容错则降低对个别储存资源不必要的依赖。

5.11 恶意程式防护

Cyberhood 将 Clam AntiVirus（ClamAV）扫描整合至资讯保护架构。档案在加密与储存前先进行病毒扫描，使资讯进入受保护储存之前即具备一层恶意程式侦测。

5.12 入侵与勒索软体防护

Cyberhood SPAN 将高度加密的分散式储存与多个独立存取屏障结合。若要直接存取实际档案，必须通过多个彼此独立的存取控制层。

单一装置遭入侵本身并不足以取得原始档案内容。使用者电脑上的勒索软体若未取得合法身分验证，无法直接控制 SPAN 中的档案。

这些机制应被理解为多层式架构防护，而不是对所有安全事件的绝对保证。

5.13 安全与容错

安全与可用性密切相关。储存资源可能因设备故障、实体损坏或恶意活动而无法使用。

Cyberhood SPAN 透过分散式储存与容错机制处理此关系。损坏或不可用的设备可被隔离，并在设备替换或执行复原程序后恢复设定的保护条件。

5.14 安全与分散式架构

Cyberhood 的安全模型与其分散式架构密不可分。平台将基础架构、服务、资讯、储存、安全边界与存取控制分布于多个架构层次。

5.15 安全与企业协作

企业协作会持续产生资讯交换。

Cyberhood 在同一平台环境中提供私人讯息、档案分享、专案协作、工作流程与企业应用。

Cyberhood Messenger 架构提供一对一与群组通讯，并支援文字、图片、影片及档案交换。

企业导向的通讯，使组织能对企业环境中的人员、通讯管道与交换资讯保有更高程度的管理能力。

这形成一项架构优势：

- 通讯、协作、身分、授权与资讯保护可在共同的企业环境中运作。

5.16 安全稽核与管理控制

安全不仅需要预防，也需要可视性与管理监督。Cyberhood 企业服务可保留活动纪录，以支援稽核或监督用途，而对这些资讯的存取仍由系统控制。

因此，安全管理涵盖身分、存取控制、资讯保护、活动纪录与管理监督。

5.17 多层式企业安全模型

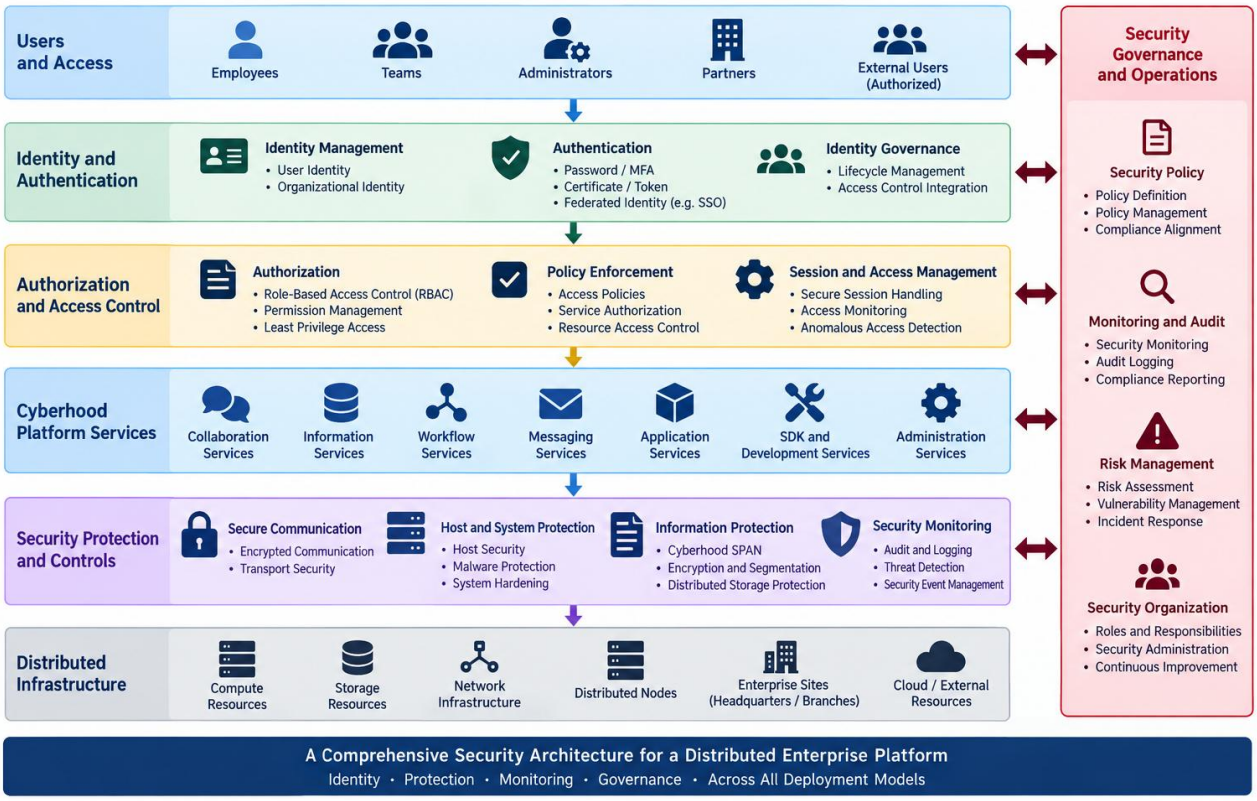


图 5-1 — 安全架构模型

Cyberhood 安全架构可表示为多层式模型：企业应用与协作位于身分与授权、恶意程式防护、SPAN 加密储存、分散式基础架构、安全通讯及 Independent Firewall 防护之上，并与这些能力形成架构关系。

关键架构原则

- 多层防御 — 企业安全由多种互补的防护机制共同建立。
- 以身分为核心的存取 — 资源存取与使用者帐号及组织角色相关联。
- 分散式防护 — 安全机制延伸至分散式基础架构，而非仅依赖中央网路周界。
- 受保护资讯 — 企业资讯透过授权、加密、分散式储存及相关控制受到保护。
- 储存前恶意程式检查 — 档案可在进入受保护加密储存前先进行扫描。
- 存取层分离 — 受保护资讯透过身分验证、授权与分散式储存架构，与端点直接存取分离。
- 具容错能力的保护 — 资讯保护纳入容错与复原机制。
- 管理可视性 — 活动纪录可支援企业服务中的稽核与监督。

重点摘要

- Cyberhood 将安全视为架构能力，而不是单一产品功能。
- 安全网路通讯是基本的安全层。
- 分散式主机可透过 Independent Firewall 受到保护。
- 组织帐号提供权限管理的基础。
- 使用者帐号可对应一个或多个组织角色。
- 授权将组织身分与资源存取连结。
- Cyberhood SPAN 为安全架构加入加密分散式储存。
- 档案会在加密与储存之前进行恶意程式扫描。
- 分散式加密储存可在遭入侵端点与受保护资讯之间提供额外隔离。
- 容错与复原有助于提升资讯韧性。
- Mail 与 Messenger 等企业服务运作于更广泛的安全架构之中。
- 管理活动纪录可支援稽核与监督。

摘要

Cyberhood 企业安全架构以多层式防护模型为基础。

此架构结合安全通讯、透过 Independent Firewall 实现的分散式主机防护、身分、授权、资讯保护、恶意程式防护、分散式加密储存、容错与复原。

Cyberhood 并非依赖单一安全边界，而是将防护分布于基础架构、平台、资讯与应用层。

Cyberhood SPAN 进一步将加密分散式储存与容错、复原、恶意程式扫描及多重存取控制屏障结合，以强化此模型。

其结果是一套不仅保护网路周界，更以保护整体企业资讯环境为目标的安全架构。

PART III — 企业平台

第 6 章

企业协作平台

执行概述

Cyberhood 提供企业协作能力，连结组织帐号、即时通讯、邮件、行事历、工作管理、公告、档案空间、分享、版本控制、搜寻及跨平台档案存取。

协作是 Cyberhood 分散式企业平台的原生能力；通讯、资讯管理、工作空间组织、分享与保护，皆以彼此连结的平台能力运作。

6.1 协作作为原生平台能力

Cyberhood 透过组织身分、授权、工作空间、资讯服务与受保护储存，将协作与资讯管理整合。因此，协作是平台架构的一部分，而不是一组彼此独立的通讯工具。

协作架构可摘要为：

- 身分 + 通讯 + 工作空间 + 分享 + 资讯管理 + 协作

6.2 组织身分

身分是企业协作的基础。使用者透过组织帐号参与平台，而权限与角色则决定其与企业资源之间的关系。

此以身分为核心的模型，为通讯、档案、工作空间与企业应用中的协作提供一致基础。

6.3 企业通讯

通讯是企业协作的基本组成。Cyberhood 透过 Mail 与 Messenger 提供通讯能力，使组织可在企业平台内维持通讯。

6.4 企业即时通讯

Cyberhood Messenger 提供一对一与群组通讯，并支援文字、图片、影片及档案交换。此通讯模型同时支援个人之间的直接通讯与群组成员间的沟通。

6.5 企业邮件

Cyberhood Mail 在平台内提供企业电子邮件能力。电子邮件与组织帐号相关联，并在企业资讯环境中运作。

6.6 企业工作空间模型

Cyberhood 将协作整合至四种资讯空间：我的空间（My Space）、公共空间（Public Space）、我分享的空间（Sharing With Space）与分享给我的空间（Shared From Space）。这些空间依资讯所有权与分享关系加以区分。

此模型建立清楚的资讯分享方向，区分个人管理资讯、供较广泛组织成员存取的资讯、使用者分享给他人的资讯，以及他人分享给使用者的资讯。

6.7 我的空间（My Space）

我的空间提供与使用者个人工作空间相关的个人资讯环境，作为该使用者在整体授权架构下管理资讯的位置。

6.8 公共空间（Public Space）

公共空间提供较广泛组织成员存取的资讯环境，用以区分组织可用资讯与个人工作空间内维护的资讯。

6.9 我分享的空间（Sharing With Space）

我分享的空间代表使用者分享给其他使用者或组织参与者的资讯，清楚呈现资讯由使用者工作空间向外分享的关系。

我分享的空间 → 我分享给其他人的资讯

6.10 分享给我的空间（Shared From Space）

分享给我的空间代表其他使用者或组织参与者分享给该使用者的资讯，清楚呈现透过组织资讯分享关系所接收的资讯。

我分享的空间 → 我分享给其他人的资讯

分享给我的空间 → 其他人分享给我的资讯

此区分使分享资讯的来源与方向更容易理解，并为企业资讯管理建立更清楚的基础。

6.11 档案管理与协作

档案管理是企业协作的基本组成。Cyberhood 将档案管理与工作空间组织、分享、版本控制、搜寻、授权及受保护储存连结。

企业资讯生命周期可理解为：建立 → 储存 → 分享 → 协作 → 版本化 → 搜寻 → 保护。

6.12 版本控制

协作资讯会随时间持续变化。Cyberhood 将版本控制能力纳入资讯管理架构；其协作模型包含 Concurrent Read Concurrent Write（CRCW）与 Concurrent Read Exclusive Write（CREW）模式，以支援版本控制情境。

6.13 全文搜寻

Cyberhood 提供全文搜寻能力以支援资讯探索。目录、档案摘要与文件说明可纳入全文索引，以支援关键字资讯检索。

6.14 跨平台存取

Cyberhood 平台支援 Windows、Linux、macOS、iPhone、Android 及网页浏览器环境的桌面与行动存取模式。

6.15 同一环境中的通讯与资讯

Cyberhood 将通讯与资讯连结于同一企业环境。使用者可透过 Mail 与 Messenger 沟通，同时在平台中处理档案、工作空间、分享资讯及组织资源。

6.16 协作与企业工作管理

Cyberhood 的协作环境包含行事历、工作与公告栏功能，以支援组织通讯及日常协调。

6.17 协作与安全

Cyberhood 将协作与身分、授权、受保护储存，以及第 5 章所述的多层式安全架构连结。

身分 → 授权 → 协作 → 资讯保护

6.18 协作与 SPAN

Cyberhood SPAN 在协作环境之下提供 Protected Information Layer。因此，档案管理与协作会与受保护分散式储存形成架构关系。

6.19 分散式平台上的协作

Cyberhood 的协作环境运作于分散式平台基础之上。此架构连结分散式基础架构、分散式平台服务、协作与资讯服务、企业应用及商业服务。

6.20 企业协作模型

完整的 Cyberhood 协作模型，将企业使用者与组织身分连结至 Mail、Messenger、工作空间、资讯服务、分享、版本控制、搜寻与受保护储存。

关键架构原则

- 协作作为原生能力 — 协作整合于 Cyberhood 平台之中。
- 以身分为核心的协作 — 使用者透过组织身分与权限参与。
- 以工作空间为基础的资讯管理 — 不同工作空间模型支援不同的资讯所有权与协作需求。
- 具方向性的资讯分享 — 我分享的空间与分享给我的空间，区分向外分享的资讯与从他人接收的资讯。
- 整合式通讯 — Mail 与 Messenger 在企业环境内提供通讯能力。
- 资讯连续性 — 档案、分享、版本控制与搜寻形成连续的资讯生命周期。
- 跨平台可存取性 — Cyberhood 平台支援桌面、行动与浏览器环境。
- 受保护的协作 — 协作与身分、授权及受保护资讯连结。
- 分散式协作 — 协作运作于更广泛的分散式平台基础之上。

重点摘要

- Cyberhood 提供整合式企业协作环境。
- 协作连结身分、通讯、资讯、工作空间、分享与保护。
- Mail 与 Messenger 提供核心企业通讯能力。
- 我的空间、公共空间、我分享的空间与分享给我的空间，提供不同的资讯分享模型。
- 我分享的空间用以识别使用者分享给其他人的资讯。
- 分享给我的空间用以识别其他人分享给使用者的资讯。
- 版本控制支援资讯可追溯性。
- 全文搜寻支援资讯探索。
- 行事历、工作与公告栏功能支援组织协调。
- 跨平台存取支援桌面、行动与浏览器环境。
- SPAN 在协作环境之下提供受保护储存层。

摘要

Cyberhood 企业协作平台将通讯、资讯管理、工作空间、分享、版本控制、搜寻及跨平台存取整合于共同的分散式企业环境。

第 7 章

企业应用生态系统与整合

执行概述

Cyberhood 提供整合式企业应用环境，使专业化企业应用在共享的分散式平台架构上运作。企业资讯入口（EIP）、工作流程／电子签核、ERP、CRM、专案管理、通讯与协作及其他企业应用，各自保留其专业化业务责任，同时参与协调式企业环境。

Cyberhood 企业应用整合是一项已实作的平台能力。API Integration、Transaction Orchestration、Enterprise Service Bus（ESB）、Message Bus、Automatic Cross-Application Synchronization，以及共享的工作流程／电子签核机制，连接参与应用之间的功能、交易、讯息、资讯流与企业流程。

此架构同时在平台层与企业流程层整合专业化能力。应用可交换资讯、协调交易、参与跨应用工作流程、同步相关应用状态，并使用共同平台服务，而不需要将各自的专业化业务责任合并成单一巨型应用。

因此，专业化与整合可以共存：企业应用维持专业分工、企业流程受到协调、资讯保持同步，而平台服务维持共享。

7.1 从应用组合走向整合式企业架构

Cyberhood 将分散式企业平台从基础架构与共享平台服务延伸至整合式企业应用环境。EIP、工作流程／电子签核、ERP、CRM、专案管理、通讯与协作及其他企业应用，以专业化业务能力运作，同时参与共同的分散式企业架构。

架构目标不是将专业化企业应用合并为单一巨型系统，而是透过已实作的企业整合能力，连接其 API、交易、讯息、资讯流与企业流程，使每个应用保留自身业务责任，同时参与协调式企业营运。

Cyberhood 因此将企业应用整合视为平台能力，而不是彼此孤立的点对点连线集合。

企业应用整合不要求功能趋同。

企业应用维持专业化；企业流程受到协调；资讯保持同步；平台服务维持共享。

7.2 企业应用整合架构

Cyberhood 企业应用整合架构由一组彼此关联的架构责任构成。企业应用提供专业化业务功能；共享工作流程与企业流程机制跨越应用边界协调组织程序；企业整合服务提供 API 交换、交易编排、服务与讯息通讯，以及跨应用自动同步等已实作机制；Cyberhood Platform Core Services 提供共同的身分、授权、资讯、协作、通讯、管理与安全关系；Cyberhood SPAN 为适用资讯提供受保护资讯层；分散式基础架构则提供底层运算、储存、网路、站点、边缘、资料中心与云端资源。

企业使用者与组织环境 → 专业化企业应用 <-> 共享企业流程与工作流程整合 <-> 企业整合服务 <-> Cyberhood Platform Core Services <-> Cyberhood SPAN <-> 分散式基础架构

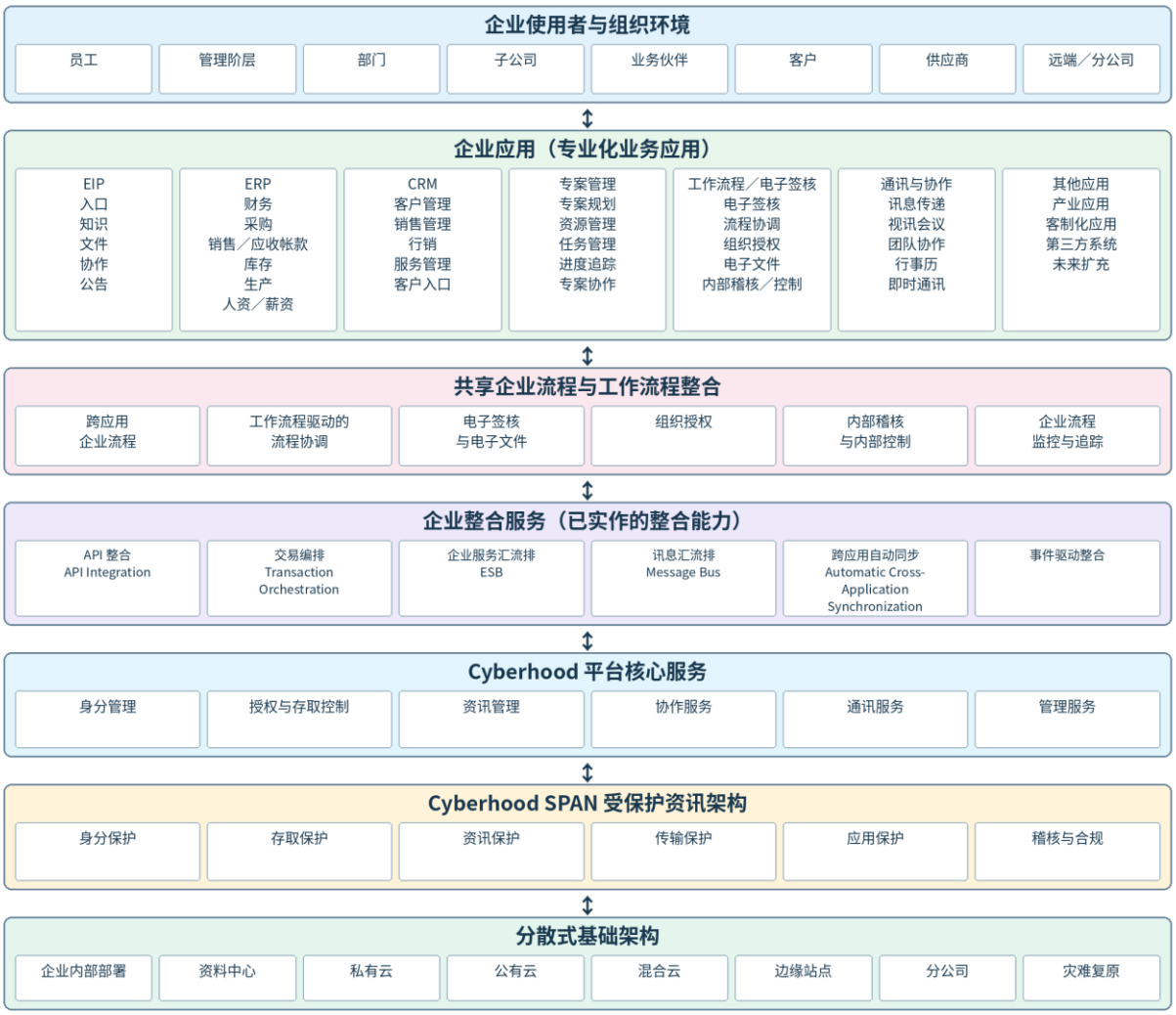


图 7-1 Cyberhood 企业应用整合架构

透过共享工作流程、企业整合服务、共同平台服务、Cyberhood SPAN 与分散式基础架构整合专业化企业应用

图 7-1 — Cyberhood 企业应用整合架构

图 7-1 所呈现的关系对应 Cyberhood 已实作的功能能力。专业化企业应用透过 API Integration、Transaction Orchestration、ESB、Message Bus、Automatic Cross-Application Synchronization、共同平台服务、受保护资讯架构与分散式基础架构，参与共享工作流程与企业流程。

7.3 专业化企业应用

Cyberhood 在应用层保留专业化，因为不同企业责任需要不同的业务逻辑、资讯模型与营运流程。整合的目的在于连接责任，而不是消除责任边界。

企业资讯入口（EIP）— 提供组织资讯与工作环境，让使用者存取企业资讯、服务与应用能力。

工作流程／电子签核 — 支援结构化组织流程，同时作为跨应用流程协调能力。

ERP — 支援销售与应收帐款、采购与应付帐款、会计、资产与资金、库存与成本分析、生产与排程、人力资源与薪资、预算，以及外包工程／劳务支出管理。

CRM — 支援客户互动、客户资讯、服务历程、问题、产品回馈及相关客户活动。

专案管理 — 支援专案规划、执行、协调、进度管理、专案资讯与协作。

通讯与协作 — 透过企业通讯与协作工作能力连接人员、资讯与业务活动。

其他企业应用 — 可透过 Cyberhood 提供的整合机制参与整合式环境。

业务责任各自专业化；平台服务共享。

7.4 已实作的企业整合服务

Cyberhood 提供已实作的企业整合服务，在功能、交易、讯息、资讯与企业流程层级连接专业化应用。这些能力是实际企业应用环境的一部分，而不只是概念性的整合模型。

7.4.1 API Integration

API Integration 透过已定义的应用介面，使参与的应用与服务交换功能能力与资讯，在不将专业功能合并至同一应用的前提下提供整合路径。

7.4.2 交易编排（Transaction Orchestration）

Transaction Orchestration 协调跨越应用边界的业务活动。源自一个应用的交易可参与涉及其他应用的工作流程、授权、控制、处理与同步序列。

7.4.3 Enterprise Service Bus（ESB）

Cyberhood ESB 提供共享的企业整合机制，使服务与应用参与协调式互动，降低对孤立应用对应用关系的依赖，并支援共同整合架构。

7.4.4 Message Bus

Message Bus 支援参与应用与平台元件之间的讯息式通讯，使讯息与流程事件可参与跨应用处理，而不要求所有功能在单一应用中执行。

7.4.5 Automatic Cross-Application Synchronization

Automatic Cross-Application Synchronization 维持参与应用之间相关资讯与流程状态的关系。当整合式企业流程改变资讯或到达定义的流程状态时，可在整合环境中同步对应的应用关系。

API Integration → Transaction Orchestration → 讯息与服务交换 → 流程协调 → Automatic Cross-Application Synchronization

7.5 工作流程作为跨应用流程协调机制

工作流程／电子签核既是专业化企业应用能力，也是 Cyberhood 企业应用环境中的跨应用流程协调机制。

来自 ERP、CRM、专案管理、EIP 或其他整合应用的业务事件与交易，可启动、参与或回应工作流程驱动的程序。工作流程提供共享流程关系，使应用所产生的活动能经过电子签核、电子文件、组织授权、内部稽核、内部控制与后续业务处理。

透过 API Integration、Transaction Orchestration、ESB、Message Bus 与 Automatic Cross-Application Synchronization，工作流程状态与结果可参与相关应用后续处理。

工作流程不只是核准交易 — 它连接跨企业应用的业务流程。

7.6 电子签核、内部稽核与内部控制

电子签核为整合式企业流程提供结构化的组织决策机制。它不只是独立的签核应用，而可参与由企业应用启动的流程，并将核准、驳回或完成等流程状态交付后续业务处理。

内部稽核与内部控制透过工作流程／电子签核引擎连接企业营运，使稽核与控制要求可与业务交易、组织授权、佐证文件、流程纪录及后续应用处理建立关联。

业务活动 → 工作流程／电子签核 → 组织授权 → 内部控制／内部稽核 → 后续业务处理 → 跨应用同步

例如，采购活动可源自 ERP，进入电子签核流程，经过必要的组织授权与控制程序，保留相关流程纪录与佐证文件，再继续进入 ERP 或相关应用的后续处理。工作流程负责协调流程，而不取代 ERP 的专业化责任。

7.7 跨应用企业流程范例

同一套整合架构可支援跨越不同专业化应用的企业流程。以下关系用以说明架构模式，而不重新定义参与应用的责任。

ERP 交易 → 工作流程／电子签核 → 授权与控制 → 后续 ERP 处理 → 与参与应用同步。

CRM 活动 → 工作流程或相关组织流程 → 授权／协作 → 后续客户或企业处理。

专案活动 → 工作流程／电子签核 → 组织授权 → 专案处理与相关资讯同步。

EIP 使用者活动 → 应用或工作流程服务 → 企业处理 → 资讯与状态回到整合式工作环境。

应用拥有专业化业务责任；整合架构连接企业流程。

7.8 企业资讯入口（EIP）

EIP 提供组织资讯与工作环境，使企业使用者可存取资讯、应用、协作能力与企业流程。在整合架构中，EIP 可作为面向企业使用者的入口环境，而底层应用责任仍分布于专业化应用与共享平台服务。

此关系使使用者体验可以在组织层面统一，而不要求底层企业应用在功能上变得相同。

7.9 客户关系管理（CRM）

CRM 保留客户导向活动与资讯的责任。当需要组织工作流程、企业资讯、协作或后续业务处理时，客户互动、服务历程、问题、产品回馈与相关客户流程可参与更广泛的整合架构。

CRM 整合因此在保留 CRM 专业化业务能力的同时，连接客户责任与企业流程。

7.10 企业资源规划（ERP）

ERP 保留企业资源与营运流程的责任。Cyberhood ERP 环境包括销售与应收帐款、采购与应付帐款、会计、资产与资金、库存与成本分析、生产与排程、人力资源与薪资、预算，以及外包工程／劳务支出管理。

在整合架构中，ERP 交易可参与工作流程、电子签核、交易编排、讯息交换与跨应用同步，使营运交易成为组织流程的一部分，而不将底层 ERP 责任移转至工作流程或整合层。

ERP 拥有营运交易；工作流程协调组织程序；整合服务连接参与系统。

7.11 专案管理

专案管理保留专案导向规划与执行责任。当专案工作需要组织授权或与其他企业应用互动时，专案活动可参与共享工作流程、签核、协作、资讯管理与整合服务。

因此可连接专案流程与企业营运，而不要求专案管理重复 ERP、CRM 或工作流程的责任。

7.12 整合流程中的通讯与协作

整合式企业流程同时涉及人员与系统。Cyberhood 通讯与协作能力提供人员互动环境，使使用者能沟通、交换资讯并参与业务活动。

协作可与工作流程及企业应用共同运作，使组织通讯与业务处理保持连结，而不是形成彼此分离的资讯孤岛。

7.13 共同平台服务

企业整合运作于共同的 Cyberhood Platform Core Services 之上。身分与授权决定谁可参与应用与流程；资讯服务管理企业资讯关系；通讯与协作服务连接使用者与活动；管理与安全服务提供共同的平台层控制。

共享平台服务可降低每个企业应用各自建立独立架构基础的需求。

专业化应用 → 共享企业流程 → 企业整合服务 → 共同平台服务 → 分散式基础架构

7.14 企业应用整合与 Cyberhood SPAN

企业应用整合与受保护资讯架构彼此相关但在架构上不同。整合决定应用、交易、讯息与企业流程如何互动；Cyberhood SPAN 决定套用 SPAN 保护的资讯如何分段、加密、分散配置、重建并恢复至所需保护状态。

因此 SPAN 不取代企业应用整合，企业应用整合也不取代资讯保护。当应用资讯采用 SPAN 保护时，两者共同参与更广泛的 Cyberhood 平台架构。

应用整合 ≠ 资讯保护 — 两者共同参与同一企业架构。

7.15 企业应用整合与分散式基础架构

整合式企业应用不要求所有应用功能、资讯或基础架构资源位于同一实体位置。Cyberhood 分散式平台架构允许企业应用环境依部署模式跨参与的基础架构运作。

因此，应用之间的逻辑整合关系与支援它们的应用及基础架构资源之实体配置是不同的架构责任。

应用整合定义业务与服务关系；部署定义参与资源在何处运作。

7.16 企业应用整合与安全

跨应用整合仍受 Cyberhood 安全架构约束。当企业流程跨越应用边界时，身分、验证、授权、安全通讯、平台安全控制与受保护资源关系仍持续适用。

身分 → 验证 → 授权 → 整合式企业流程 → 受保护资源

7.17 整合式应用环境的架构价值

Cyberhood 企业应用整合的架构价值，在于无须要求功能趋同即可连接专业化应用。应用可依自身业务责任演进，同时持续参与共同的流程、整合、平台、资讯与基础架构关系。

已实作的 API Integration、Transaction Orchestration、ESB、Message Bus 与 Automatic Cross-Application Synchronization，使应用专业化与企业协调得以共存。

整合不要求一致化。

专业化应用可以演进，而共享平台架构维持一致。

7.18 企业应用整合模型

Cyberhood 企业应用环境可概括为从专业化业务能力走向协调式企业营运的演进：

专业化应用 → API 与讯息整合 → Transaction Orchestration → 工作流程与流程整合 → 资讯同步 → 组织协调 → 企业营运

此模型连接企业应用、组织流程、企业资讯、平台服务与分散式基础架构，同时维持清楚的架构责任。

7.19 关键架构原则

企业应用整合是 Cyberhood 已实作的平台能力。

企业应用依其业务责任维持专业化。

工作流程／电子签核提供跨应用流程协调。

内部稽核与内部控制透过工作流程／电子签核引擎参与企业流程。

API Integration 连接应用功能与资讯。

Transaction Orchestration 协调跨应用边界的业务活动。

ESB 与 Message Bus 提供共享的服务与讯息整合机制。

Automatic Cross-Application Synchronization 维持相关资讯与流程状态关系。

共同平台服务提供共享架构基础。

Cyberhood SPAN 在套用 SPAN 保护时提供受保护资讯架构。

分散式基础架构提供整合环境运作所需的实体资源。

7.20 结论

Cyberhood 企业应用整合将专业化企业应用组合转化为协调式企业应用环境。ERP、CRM、EIP、专案管理、工作流程／电子签核、通讯与协作及其他应用保留专业化责任，同时参与共享企业流程与共同平台关系。

已实作的整合架构透过 API Integration、Transaction Orchestration、ESB、Message Bus 与 Automatic Cross-Application Synchronization，连接 API、交易、讯息、资讯流、工作流程状态与应用资料关系。

此架构使 Cyberhood 能在不强迫应用进入单一巨型功能模型的情况下连接企业应用。专业化应用维持专业化；平台提供共同运作所需的机制。

专业化应用 — 整合式流程 — 共享平台服务 — 一个企业架构。

Cyberhood 不只是将企业应用放在共同平台上，而是在共享企业架构中整合其 API、交易、讯息、资讯流与企业流程。

第 8 章

开发者平台与分散式应用框架

执行概述

Cyberhood 分散式企业平台不仅提供基础架构、协作服务与企业应用，也旨在建立分散式企业应用的共同开发基础。

Cyberhood SDK 提供分散式系统应用程式设计框架，使应用可与平台的分散式服务及企业资源形成架构关系。在此架构中，应用开发与底层分散式基础架构的复杂性分离。用户端应用可专注于呈现与使用者互动，而伺服器端服务则在分散式平台环境中执行应用逻辑与处理。

因此，开发者架构可概括为：应用程式 → Cyberhood SDK → 分散式平台服务 → 分散式基础架构。

此模型使 Cyberhood 从一组企业能力，进一步延伸为可扩充的分散式应用平台。

8.1 Developer Platform 作为架构层

企业平台必须随组织需求变化而持续演进。

标准化企业应用可处理常见营运需求，但组织也可能需要专用应用、新的业务流程，或针对特定产业与营运环境设计的应用服务。

Cyberhood 透过建立在同一分散式架构上的 Developer Platform 回应此需求，而该架构亦支撑整体 Cyberhood 环境。

Developer Platform 建立以下关系：开发者 → 应用程式 → 平台服务 → 分散式资源。

Cyberhood 不将应用开发视为独立的技术环境，而是将其置于分散式平台架构之中。

因此，新应用可透过明确的架构路径，与既有企业服务共同运作。

8.2 Cyberhood SDK

Cyberhood SDK 提供分散式平台的应用开发介面。其目的在于提供开发者一套共同框架，用以依据 Cyberhood 的分散式资料处理架构开发应用。

在概念上，SDK 在应用开发与底层分散式环境之间建立抽象层：

应用程式 → Cyberhood SDK → 分散式平台服务 → 分散式基础架构

因此，应用是透过平台架构与分散式环境互动，而不是只以单一独立伺服器为设计中心。

此一区别是 Cyberhood 开发者模型的核心。

8.3 分散式应用框架（Distributed Application Framework）

传统企业应用经常围绕预先指定的伺服器或固定的基础架构关系设计。

Cyberhood 导入分散式应用模型，使应用执行与分散式平台资源形成关系。

此框架可由四个架构元素理解：身分 + 服务选择 + 应用处理 + 分散式资源。

这些元素建立一套开发模型，使应用可参与 Cyberhood 分散式环境。

由此形成的架构，将应用体验与个别基础架构资源的实体位置分离。

8.4 分散式身分验证

身分是 Cyberhood 的基础平台能力。

如前述章节所建立，组织帐号是验证、授权、协作及存取企业资讯的基础。Developer Platform 将此身分关系延伸至分散式应用执行。

概念上的应用存取顺序可表示为：使用者 → 身分验证 → 应用服务 → 企业资源。

在存取应用服务与受保护资源之前，身分验证先建立使用者与分散式平台之间的关系。

因此，应用执行可运作于 Cyberhood 全平台共同使用的身分架构之中。

8.5 分散式服务选择

Cyberhood 分散式应用模型的重要特性之一，是可依平台架构选择适当的分散式服务资源。

分散式身分验证流程可依平台模型辨识适当的分散式主机，包括较接近或效能较佳的主机，以支援应用执行。

概念上可表示为：使用者／用户端 → 身分验证 → 分散式服务选择 → 分散式主机 → 应用服务。

此架构降低应用与单一预先指定应用主机之间的概念性依赖。

服务选择机制成为分散式平台关系的一部分，而不是特定应用对基础架构的假设。

8.6 用户端与伺服器端的应用责任

Cyberhood 应用模型区分伺服器端应用处理，以及用户端的呈现与互动。此分离建立两项主要应用责任。

用户端责任主要著重于使用者呈现、使用者互动、应用介面行为，以及与应用服务的通讯。

伺服器端责任主要著重于应用逻辑、应用处理、与平台服务互动，以及应用相关资讯的处理。

其关系可表示为：用户端呈现与互动 ↔ 伺服器端应用逻辑与处理。

此分离为分散式应用开发提供清楚的架构模型。

8.7 分散式应用处理

在 Cyberhood 架构中，应用处理并非独立于分散式平台之外。伺服器端应用处理与分散式平台服务及基础架构资源形成关系。

概念上可表示为：用户端 → 应用介面 → 分散式应用服务 → 应用处理 → 平台资源。

因此，分散式平台提供应用服务运作所需的执行基础。

这使 Developer Framework 能与更广泛的 Cyberhood 分散式架构保持一致。

8.8 共用平台服务

在 Cyberhood 环境中运作的应用，可在架构上与共用平台服务连结。Cyberhood 架构框架（Cyberhood Architecture Framework, CAF）定义的分散式平台能力包括身分验证、授权、索引、分散式储存服务、工作流程、讯息传递、SDK 服务及管理。这些共用能力在应用与基础架构之间形成架构服务层。

此模型的重要意义在于架构一致性。

新应用可依循支援既有 Cyberhood 服务的同一平台基础进行设计。

8.9 资讯与储存服务

企业应用会产生、处理并使用资讯。

因此，Cyberhood 将应用开发置于更广泛的平台资讯架构中，而不是将应用资讯视为完全独立的架构领域。应用可与平台资讯及分散式储存服务形成关系。

由此建立概念关系：应用程式 → 资讯服务 → 分散式储存架构。

第 4 章所述的 Cyberhood SPAN 提供平台的受保护分散式资讯储存层。然而，此架构并不假设每一个应用或每一类应用资料都必须自动透过 SPAN 储存。

应用与受保护储存之间的具体关系，取决于应用设计及其对平台服务的使用方式。此区别维持 Developer Framework 与个别应用所采用储存实作之间的分离。

8.10 应用的安全与授权

应用扩充能力必须持续与企业安全相连。

因此，Cyberhood 将应用存取置于第 5 章所建立的身分与授权架构之中。

概念关系为：身分 → 验证 → 授权 → 应用程式 → 受保护资源。

验证确认使用者是谁。

授权决定在何种条件下可以存取资源。

应用程式提供使用者与这些资源互动所需的业务或营运能力。

此架构使应用开发与更广泛的 Cyberhood 企业安全模型保持一致。

8.11 应用与协作服务整合

第 6 章已将协作建立为 Cyberhood 分散式企业平台的原生能力。Developer Platform 进一步延伸此架构关系，提供应用与协作及资讯服务共存的基础。

此架构使协作、资讯管理与应用服务可存在于共同的分散式环境中。它也为业务流程涉及组织使用者、共享资讯、通讯或协作活动的应用提供基础。

8.12 应用与企业服务整合

第 7 章说明 Cyberhood 企业应用生态系统与整合，包括工作流程、专案管理、CRM 与 ERP。

第 8 章则透过提供额外应用与企业能力的开发框架，延伸此架构模型。

因此，其关系可表示为：既有企业应用 + 可扩充应用 → 共用分散式平台。

这并不表示每个应用都必须执行相同功能或采用相同实作。相反地，它建立共同架构基础，使不同企业应用可参与更广泛的 Cyberhood 环境。

第 7 章定义企业应用能力；第 8 章定义应用开发与扩充的架构基础。

8.13 分散式应用执行模型

Cyberhood 开发者架构可透过分散式应用执行模型加以概括。

此模型呈现数项架构原则。

第一，应用不被视为孤立的软体元件。

第二，身分提供使用者进入分散式环境的起始关系。

第三，分散式服务选择将应用执行与适当的平台资源连结。

第四，应用处理可与共享平台及资讯服务形成关系。

最终的执行模型可概括为：验证 → 选择服务 → 执行应用 → 存取平台资源。

8.14 应用扩充性

扩充性是 Cyberhood 开发者平台（Developer Platform）的核心目的。

Cyberhood SDK 与共用平台架构为新应用整合既有分散式服务与企业资源提供路径。

这表示此架构不受限于固定的一组应用。随著组织需求演进，可在分散式平台基础上开发额外的应用能力。

因此，既有应用与新开发应用都可定位于同一个更广泛的平台架构中。

这为应用的长期演进建立基础，而不需要每次导入新业务功能时，就在概念上取代底层分散式架构。

8.15 Cyberhood 作为企业应用平台

开发框架（Developer Framework）改变了 Cyberhood 的架构角色。若没有应用开发框架，Cyberhood 主要可能被视为分散式基础架构与预先定义企业应用集合的组合。

Cyberhood SDK 引入另一个架构面向：Cyberhood 成为可开发与扩充分散式企业应用的平台。

因此，架构演进可表示为：分散式基础架构 → 分散式平台服务 → Developer Framework → 企业应用 → 业务服务。

此演进将基础架构工程与应用开发及组织业务能力连结。它也在第 7 章所述的企业应用生态系统与整合架构，以及第 9 章的部署架构之间建立架构桥接。

8.16 Developer Platform 架构模型

完整的 Cyberhood Developer Platform 建立应用、SDK、共用平台服务与分散式基础架构之间的关系。

此模型可概括为：企业应用 → Cyberhood SDK → Distributed Application Framework → 身分／授权／资讯服务 → 分散式平台 → 分散式基础架构。

它也呈现 Developer Framework 在更广泛的 Cyberhood 架构框架（CAF）中的角色。

基础架构提供资源；平台服务提供共用能力；SDK 提供应用开发基础；应用则将平台能力转化为企业服务。

关键架构原则

- 分散式应用基础 — Cyberhood 提供以平台分散式系统架构为核心设计的 SDK 与应用框架。
- 应用责任分离 — 用户端呈现与互动，与伺服器端应用逻辑及处理分离。
- 身分作为应用进入点 — 分散式应用执行与 Cyberhood 身分验证形成关系。
- 分散式服务选择 — 平台模型可将应用执行与适当的分散式主机建立关联，而非假设单一预先指定伺服器。
- 共享平台服务 — 应用可与共用的身分、授权、资讯、工作流程、讯息传递、储存及管理服务形成关系。
- 安全延续性 — 应用存取持续与企业平台的身分及授权架构相连。
- 应用扩充性 — SDK 提供新应用整合分散式服务与企业资源的架构路径。
- 平台层级开发 — 应用开发成为 Cyberhood 平台架构的一部分，而非与基础架构及企业服务脱节的独立层。

重点摘要

- Cyberhood SDK 为分散式应用提供共同的开发基础。
- Developer Framework 运作于 Cyberhood 分散式基础架构与平台服务层之上。
- 分散式身分验证建立使用者与应用服务之间的关系。
- 分散式服务选择可将应用执行与适当的平台主机建立关联。
- 用户端呈现与互动，与伺服器端应用逻辑及处理分离。
- 应用可与共用平台及资讯服务形成关系。
- 身分与授权将应用存取与企业安全连结。
- 开发框架使 Cyberhood 超越预先定义的应用环境。
- 既有 Cyberhood 应用与新开发应用，可共同参与同一个更广泛的分散式平台架构。
- SDK 在分散式基础架构与可扩充企业应用之间建立架构桥接。

摘要

Cyberhood Developer Platform 与 Distributed Application Framework 将 Cyberhood 架构从基础架构、协作及预先定义的企业应用，延伸至可扩充的应用开发环境。

此架构的核心是 Cyberhood SDK，它依据平台的分散式资料处理架构提供共同的开发基础。

此框架将用户端呈现与互动，与伺服器端应用逻辑及处理分离；同时，分散式身分验证与服务选择将应用执行连结至更广泛的分散式平台。

应用可与身分、授权、资讯服务、工作流程、讯息传递、分散式资源及受保护资讯架构等共用能力形成关系。

最终的开发模型可概括为：使用者 → 验证 → 分散式服务选择 → 应用程式 → 平台服务 → 分散式资源。

透过此架构，Cyberhood 建立以下演进关系：分散式基础架构 → 平台服务 → Developer Framework → 企业应用 → 业务服务。

因此，Developer Framework 为 Cyberhood 随组织需求演进而持续扩充提供架构基础，同时维持与整个平台既有的分散式基础架构、安全、协作及企业应用模型之间的连续性。

Developer Platform 与企业整合服务

Cyberhood SDK 与 Distributed Application Framework 与第 7 章所建立的 Enterprise Integration Services 协同运作。为 Cyberhood 环境开发的应用可参与更广泛的平台架构，同时依其业务责任维持专业化。

已实作的 API Integration、Transaction Orchestration、ESB、Message Bus 与 Automatic Cross-Application Synchronization，提供参与应用交换资讯、协调交易、传递讯息与参与跨应用流程的整合机制。

SDK 与应用框架提供开发基础；Enterprise Integration Services 提供跨应用整合能力；Platform Core Services 提供共同企业服务；Distributed Infrastructure 提供参与的执行资源。

Cyberhood 不要求每个应用使用所有整合机制，也不要求所有应用资讯都采用 SPAN 保护。整合与保护依应用及部署需求套用。

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

应用开发与应用整合彼此相关，但在架构上不同。

PART IV — 架构

第 9 章

部署模式与参考架构

执行概述

Cyberhood 分散式企业平台可运作于多样化的企业基础架构环境。

企业可能在单一据点、多个办公室与营运站点、企业自主管理的基础架构、私有云，或私有与外部基础架构混合的环境中运作。

Cyberhood 提供可依这些需求调整的分散式平台架构，而不必因每一种实体拓扑重新定义企业平台。

Cyberhood 将逻辑企业平台架构与其所运作的实体基础架构拓扑分离。企业应用、协作服务、身分与授权、受保护资讯、分散式处理及平台服务维持于共同架构中；底层运算、储存、网路、节点与站点资源则可依组织需求演进。

一套平台架构 — 多种部署模式。

部署关系可表示为：企业需求 → 部署模式 → Cyberhood 平台架构 → 分散式基础架构资源。

本章涵盖私有企业、私有云、混合云、多站点企业、分散式本地节点（Distributed Local Node, DLN）及复原导向部署。这些特性不必互斥，可依基础架构策略、地理分布、营运需求、资讯保护需求及服务持续性目标组合使用。

部署决定平台资源在哪里运作；

平台架构决定企业能力如何与这些资源形成关系。

9.1 部署架构原则

分散式企业平台必须支援不同基础架构环境，而不需要为每一种部署情境重新设计企业架构。Cyberhood 透过分离逻辑平台能力与其底层实体基础架构来达成此目标。

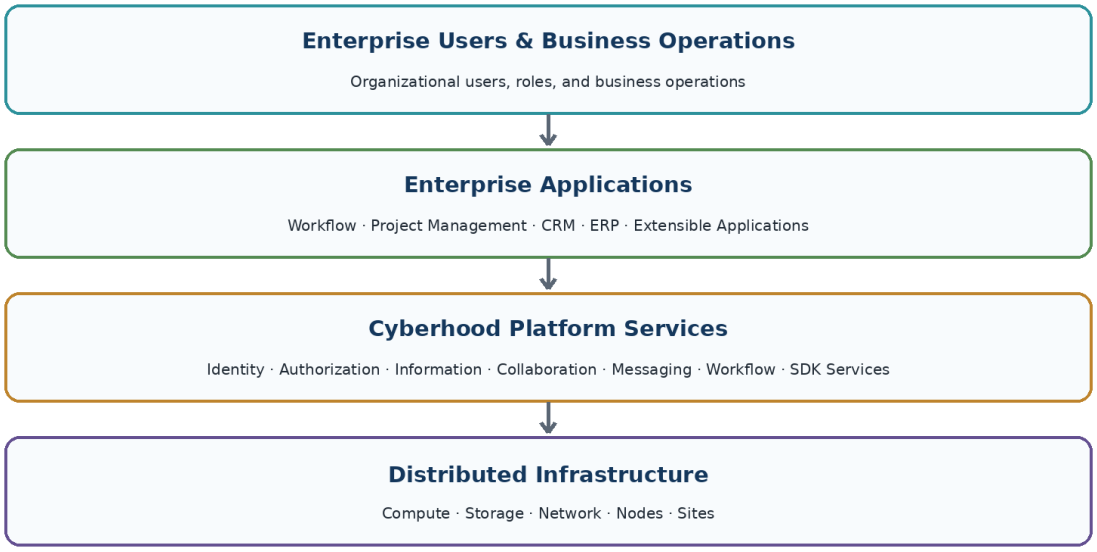


图 9-1 — Cyberhood 四层部署架构

分散式基础架构提供支援平台所需的实体和虚拟资源。 Cyberhood 平台服务在这些资源之上提供通用功能。企业应用程式利用平台基础架构来提供专门的组织功能。企业使用者和业务营运根据组织角色和营运需求与由此产生的应用程式和服务进行互动。

- 基础架构分布 — 运算、储存、网路、节点和站点可以根据部署要求进行分布。
- 平台一致性 — Cyberhood 平台服务在底层基础架构拓扑之上提供共同的架构基础。
- 应用不依赖单一基础架构位置 — 企业应用透过平台运作，而非仅由某一实体伺服器位置所定义。
- 分散式资讯资源 — 资讯服务可与分散式及受保护的储存资源形成架构关系。
- 模组化演进 — 部署容量可随组织需求变化而演进。

逻辑平台架构与实体部署拓扑彼此相关，但在架构上有所区别。

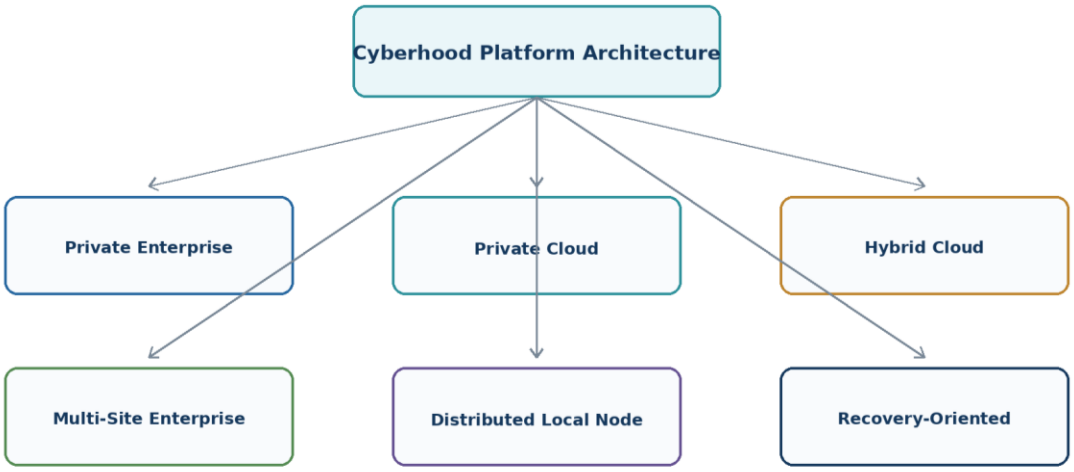


图 9-2 — Cyberhood 部署模式

9.2 私有企业部署

私有企业部署将 Cyberhood 基础架构置于组织控制的环境中，可包含企业运算、储存、内部网路、节点及其他技术资源。

Cyberhood 在此环境中提供身分、授权、协作、资讯服务、企业应用与分散式处理的共同平台基础。私有部署不要求所有资源位于同一实体地点；企业控制的资源可分布于总部、资料中心、分公司、营运设施或其他组织位置。

私有部署 ≠ 单一站点部署

私有企业部署定义的是控制环境，而不是强制性的实体拓扑。

9.3 私有云部署

私有云部署扩展了私有企业模式，它将运算、储存、网路和平台资源组织在由组织控制或专用于组织的面向云端的基础架构环境中。

私有云提供基础架构资源；Cyberhood 则提供运作于其上的分散式企业平台。

Cyberhood 的身分、授权、协作、资讯管理、企业应用与分散式处理仍属平台架构；底层则依组织私有云策略配置。本概念模型不依赖特定基础架构供应商、虚拟化平台或云端实作。

云端基础架构 ≠ 企业平台。

9.4 混合云部署

混合云部署可结合企业自主管理的基础架构与外部或云端资源，同时维持共同的 Cyberhood 平台架构。重点不是单纯将应用从一个环境搬到另一个环境，而是让适当资源依部署需求参与分散式平台。

实际网路、基础架构整合、安全控制、连线与营运设定取决于组织选择的环境；因此 Cyberhood 混合架构不依赖特定公有云供应商。

基础架构可以不同；平台架构保持一致。

混合部署本身不代表自动工作负载迁移、通用应用可携性、云原生编排或自动地理容错移转。

9.5 多站点企业部署

许多企业在多个实体地点运营，包括总部、分支机构、区域设施、营运站点和其他组织环境。 Cyberhood 的分散式架构为这些地点融入更广泛的企业平台架构提供了基础。

每个地点可以根据其营运角色、可用基础架构、分配的平台服务和部署要求参与其中。多站点架构并不要求每个地点都拥有相同的基础架构或执行相同的平台职责。

共同平台架构不要求站点架构完全一致。

多站点描述的是地理拓扑；它本身不代表 Active-Active、每站相同应用部署、全面资讯复写、自动地理容错移转或预先定义的 RPO/RTO。

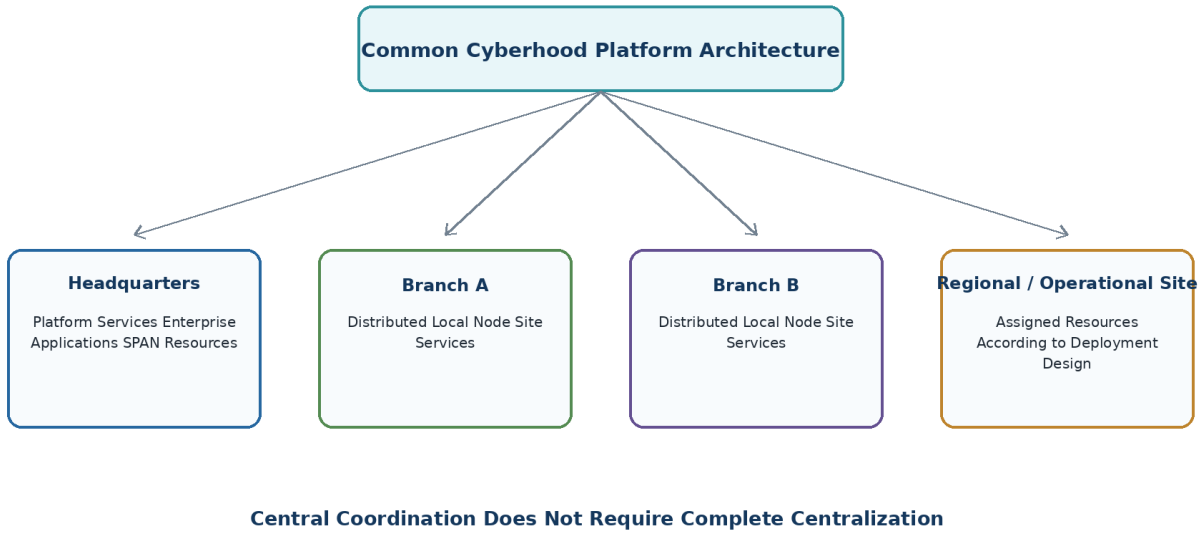


图 9-3 — 多站点企业与分散式本地节点架构

9.6 分散式本地节点部署

分散式本地节点（Distributed Local Node, DLN）提供将 Cyberhood 平台能力延伸至分散式组织据点的架构机制。DLN 可参与整体 Cyberhood 环境，并与特定站点的使用者、服务、处理需求、储存架构与基础资源形成关系。

DLN 的实际角色取决于部署设计及该站点被赋予的责任；不应解读为每个站点都必须部署完全相同的设备或服务配置。

分散式本地节点（Distributed Local Node, DLN）将平台延伸至站点；其所承担的责任取决于部署设计。

分散式本地节点 ≠ 独立的本地系统

9.7 总部与分公司架构

常见企业情境包含总部与一个或多个分公司。Cyberhood 可透过分散式架构，使中央与本地资源共同参与同一平台拓扑。

总部可承担中央平台责任、企业服务或组织资源；分公司则透过适当指派的分散式资源参与。这不表示所有 Cyberhood 服务都必须集中于总部。

集中协调不等于完全中央集中。

架构可依各站点的规模、工作负载、可用基础架构与营运角色持续演进。

9.8 地理分散架构

Cyberhood 可将分散式基础架构延伸至地理分离的总部、分公司、区域设施、营运站点、资料中心及其他环境。

地理基础架构分布

定义运算、储存、网路、节点及其他资源的实体位置。

地理服务分布

定义平台与应用服务责任在哪里运作。

地理资讯保护

定义受保护企业资讯如何透过 Cyberhood SPAN，在地理分离的储存资源之间参与资讯保护。

地理基础架构分布 ≠ 自动服务分布、

地理服务分布 ≠ 自动地理容错移转

地理资讯保护 ≠ 自动 Active-Active 服务架构

地理分散可提供降低对单一实体位置不必要依赖的架构基础，但实际运作行为仍取决于参与服务与部署设定；它不会自动建立 Active-Active 区域架构、全面复写或自动地理容错移转。

9.9 高可用性部署模型

第 3 章将高可用性（High Availability, HA）定义为包含分散式资源、故障侦测、资源隔离、重新分配、复原及容量恢复的架构能力；本章将其套用至部署拓扑。

HA 部署的目的，是降低对单一基础架构元件的不必要依赖，并建立服务持续性机制可运作的架构基础。

仅有多个资源并不构成高可用性。

HA 取决于分散式资源、故障侦测、隔离、服务或工作负载重新分配与复原之间的关系，不代表每个应用、服务或资源都具有相同可用性。

分散式部署建立 HA 基础；实际可用性取决于部署设定与参与服务。

服务配置

Cyberhood SPAN 在部署架构中提供 Protected Information Layer。企业应用与资讯服务操作逻辑企业资讯；SPAN 则管理该资讯跨参与储存资源的分散式受保护表示形式。

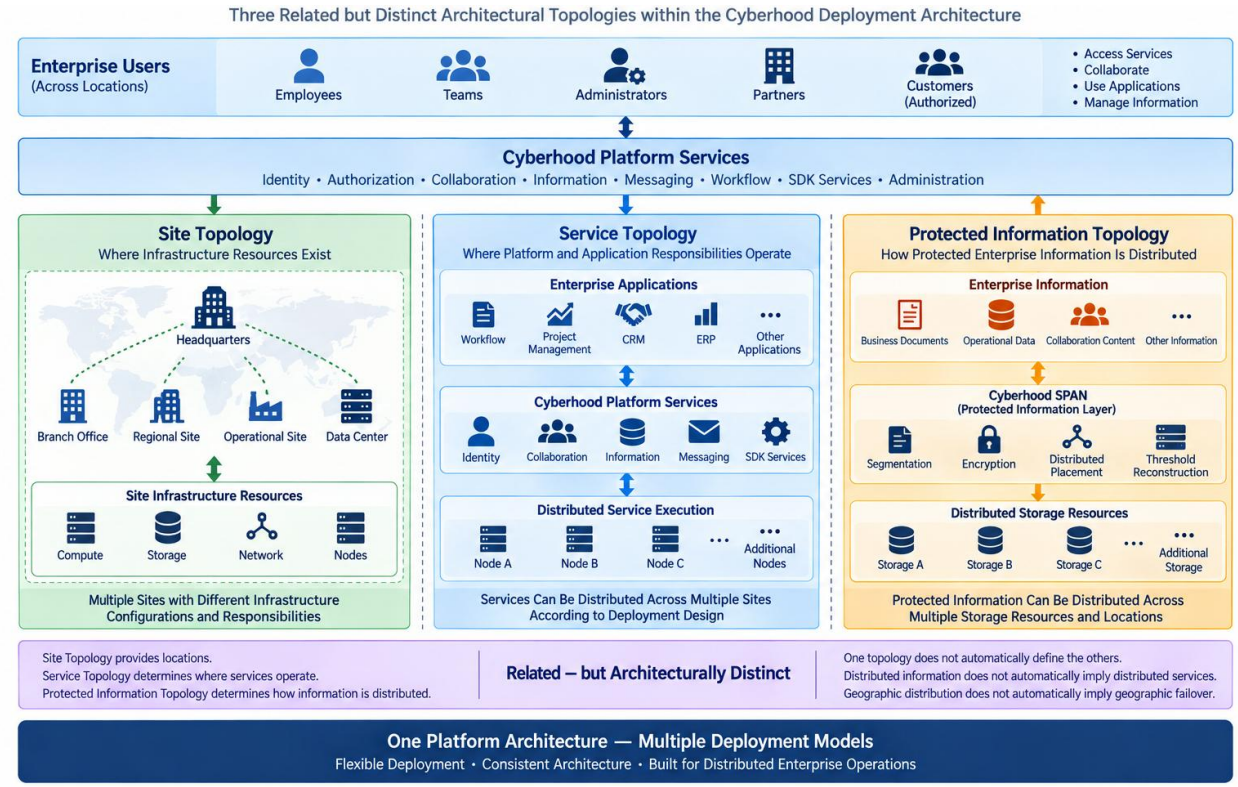


图 9-4 — 站点、服务与受保护资讯拓扑。服务配置定义平台与应用处理责任在哪里运作；受保护资讯配置定义 SPAN 资讯如何分散于参与储存资源

服务配置

定义平台与应用处理责任在哪里运作。

受保护资讯配置

定义受 SPAN 保护的资讯如何分散于参与的储存资源。

服务配置与受保护资讯配置彼此相关，但在架构上有所区别。

应用位置 ≠ 完整资讯位置

受保护资讯分布 ≠ 自动应用分布

在保护与部署设计支援的情况下，受保护资讯元件可跨地理分离的基础架构参与。地理分散的受保护资讯配置不会自动建立地理服务容错移转。

9.11 复原导向部署

高可用性与复原导向架构处理相关但不同的营运目标。高可用性主要处理参与资源或服务不可用时的服务持续性；复原导向架构则处理中断超过现行环境持续能力后的服务恢复。

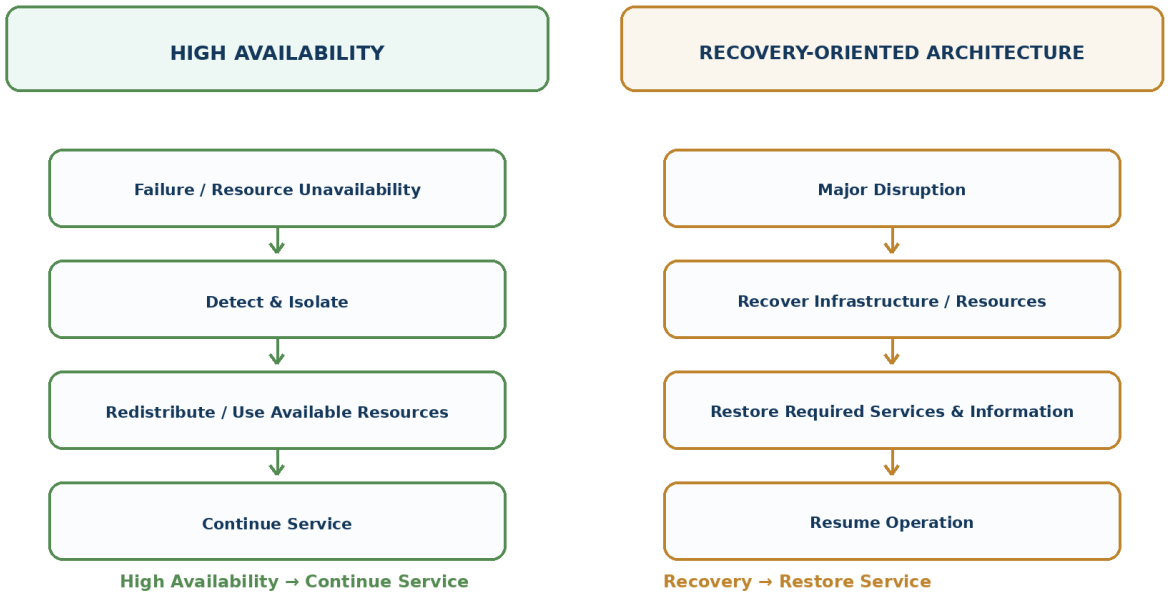


图 9-5 — 高可用性与复原导向架构

高可用性 → 持续服务；

复原导向架构 → 恢复服务。

服务持续性与复原之间的界线，取决于部署架构、参与服务、可用资源及中断性质。复原导向部署可使用分散式基础架构与地理分离资源，作为组织整体营运持续架构的一部分。

分散式架构提供复原的基础，但本身不定义复原政策。

Cyberhood 平台架构不预设通用的复原点目标（RPO）、复原时间目标（RTO）或自动灾难复原政策；这些要求必须依组织需求与实际部署设定决定。

9.12 跨部署模式的安全架构

部署拓扑可以改变，但 Cyberhood 企业安全架构的基本原则仍适用于私有企业、私有云、混合云、多站点、DLN 与复原导向环境。企业资源存取持续与身分、验证、授权、通讯保护、主机保护、恶意程式防护及受保护资讯相连。

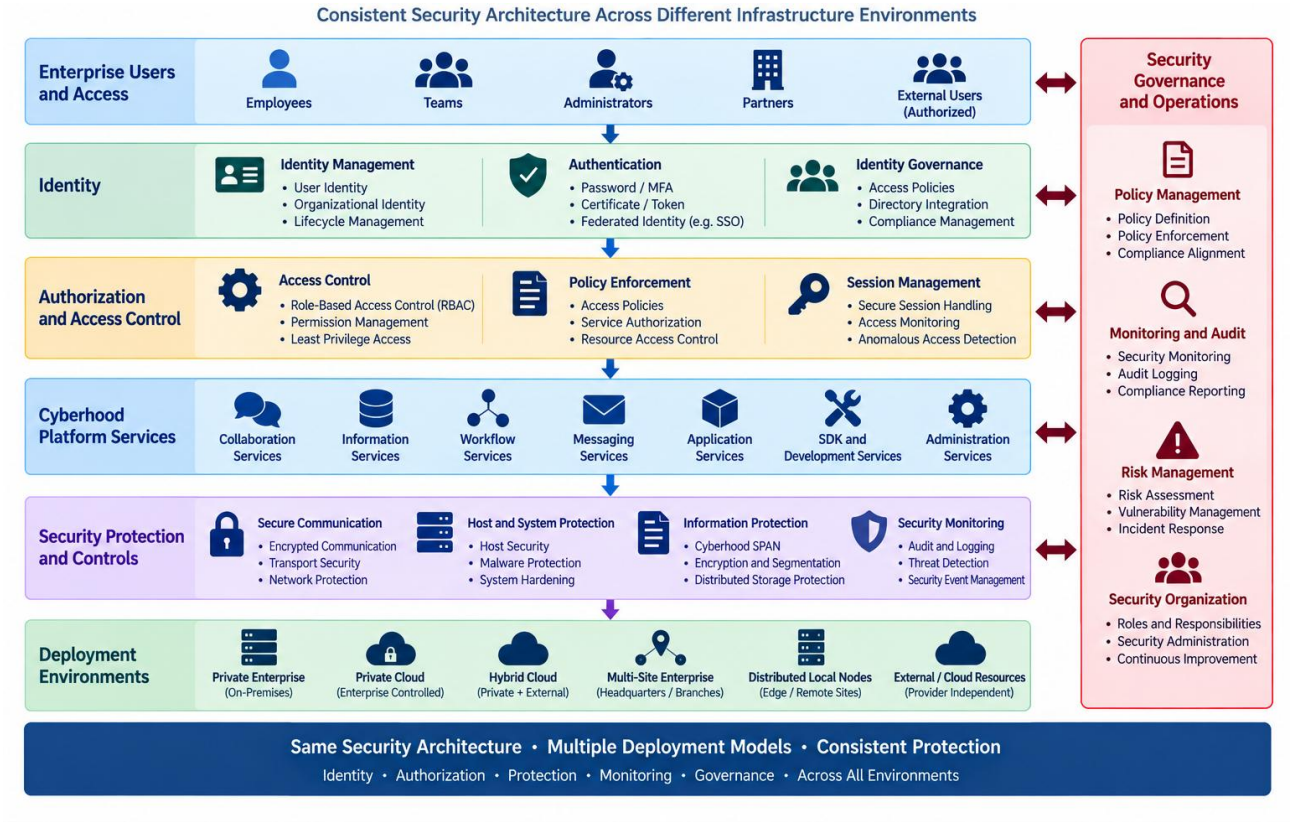


图 9-6 — 跨部署模式的安全

部署模式改变基础架构拓扑，但不取代安全架构。

安全政策与部署拓扑彼此相关，但在架构上有所区别。

分散式部署延伸安全边界，而不是消除安全边界。

9.13 跨站点企业协作

分散式组织需要不受使用者实体同站限制的协作能力。Cyberhood 提供共同平台，使不同位置的使用者可参与通讯、资讯分享、工作空间、协作及企业资讯服务。

Cyberhood 工作空间架构——包括我的空间（My Space）、公共空间（Public Space）、我分享的空间（Sharing With Space）与分享给我的空间（Shared From Space）——代表的是逻辑资讯环境，而不是实体场地边界。

工作空间是逻辑资讯环境，而不是实体站点边界。

使用者位置 ≠ 资讯位置

协作边界 ≠ 站点边界

9.14 企业应用部署

Workflow、Project Management、CRM、ERP 等企业应用运作于共同平台架构之上。其业务责任是逻辑应用责任，不应只由单一实体伺服器位置定义。

业务责任各自专业化；平台服务共享。

应用处理可依应用设计与部署设定，与分散式平台资源形成关系。应用责任是逻辑的；执行位置取决于部署设计。

应用责任属于逻辑层次；执行位置则取决于部署设计。

企业应用架构 ≠ 固定实体伺服器位置

这不代表每一个应用都会在不同资源或站点之间自动迁移。

9.15 Developer Platform 与分散式应用部署

Cyberhood SDK 与 Distributed Application Framework 提供开发基础，使额外应用可参与分散式企业架构：

应用 → Cyberhood SDK → Distributed Application Framework → 分散式平台服务 → 分散式基础架构。

身分验证建立使用者与分散式应用环境的关系；分散式服务选择可依 Cyberhood 平台模型，将应用执行与适当平台主机建立关联。应用也可与身分、授权、资讯服务、Workflow、Messaging、储存及管理服务形成关系。

分散式服务选择 ≠ 通用的自动应用容错移转。

应用扩充应维持平台架构一致性。

9.16 模组化部署扩充

企业需求会持续演进，可能增加运算能力、分散式节点、储存容量、组织据点或应用能力。Cyberhood 支援这些维度依需求模组化演进。

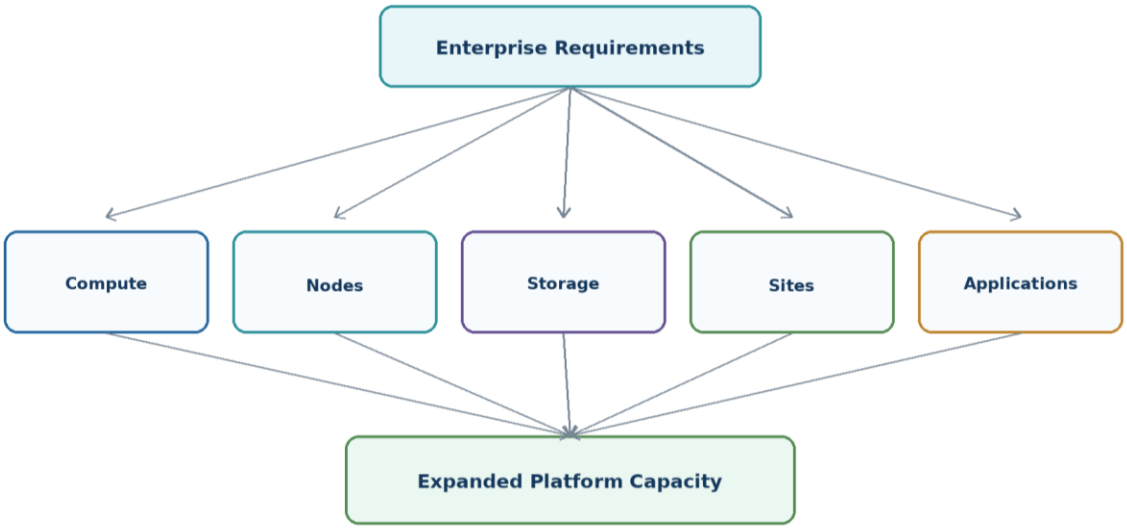


图 9-7 — 模组化部署扩充模型

模组化扩充是多维度的，而非强制循序路径：

- 运算扩充 — 增加运算资源。
- 节点扩充 — 增加参与的分散式节点。
- 储存扩充 — 增加储存容量，并在适用时增加 SPAN 参与资源。
- 站点扩充 — 增加组织据点或基础架构位置。
- 应用扩充 — 透过既有或可扩充的平台服务增加应用能力。

扩充会改变容量与拓扑，但不需要重新定义平台的基本架构。

9.17 私有企业参考架构

私有企业参考架构呈现企业控制环境中，企业使用者、企业服务、Cyberhood 平台服务、分散式资源与受保护资讯之间的逻辑关系。它是逻辑参考模型，而非强制硬体配置；节点、储存、实体系统与服务数量依组织需求决定。

企业服务运作于 Cyberhood 平台服务之上；分散式服务资源与 Cyberhood SPAN Protected Information Layer 可透过彼此相关但不同的架构路径运作于参与的运算、网路与储存资源之上。

私有企业部署定义的是控制环境，而不是强制性的实体拓扑。

9.18 多站点企业参考架构

多站点企业参考架构呈现总部、分公司及其他组织位置如何参与共同的逻辑 Cyberhood 平台。各站点可依营运角色配置不同的平台服务、企业应用、DLN、运算、储存、网路及 SPAN 参与资源。

共同平台架构不要求相同站点架构；

集中协调不要求完全中央集中。

因此，分公司不必只被视为远端使用单一中央应用环境的使用者；在适当情况下，分散式基础架构可成为更广泛企业平台拓扑的一部分。

9.19 混合企业参考架构

混合企业参考架构结合企业自主管理基础架构、分散式组织站点，以及外部或云端基础架构资源。不同来源的资源可参与分散式平台，而 Cyberhood 逻辑架构保持一致。

基础架构来源 ≠ 平台架构。

基础架构可以不同；平台架构保持一致。

此架构刻意不依赖特定公有云供应商。实际的基础架构整合、网路、安全、营运控制、服务部署与云端设定，取决于组织所选择的环境。

9.20 Cyberhood 部署架构模型

完整的 Cyberhood 部署架构整合企业营运、企业服务、共同平台能力、分散式基础架构、受保护资讯及跨层安全。

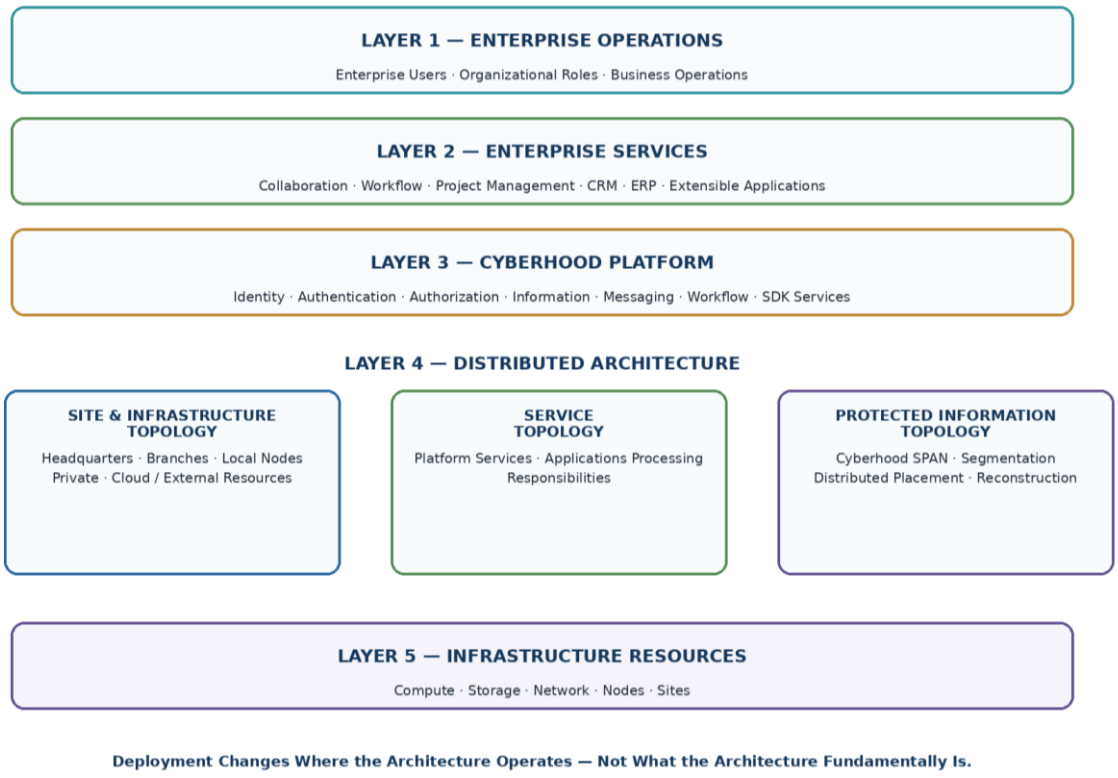


图 9-8 — Cyberhood 企业部署架构模型

此模型区分站点与基础架构拓扑、服务拓扑及受保护资讯拓扑。这些维度彼此相关，但各自具有不同的架构责任。安全则透过身分、验证、授权、安全通讯、主机防护与受保护资源，作为跨层责任贯穿整体架构。

彼此相关 — 但在架构上有所区别

私有企业、私有云、混合云、多站点企业、分散式本地节点与复原导向部署，代表 Cyberhood 整体架构因应不同企业基础架构需求的不同应用方式。

一套平台架构 — 多种部署模式

部署改变架构运作的位置，而不是架构的本质。

关键架构原则

- 一套平台架构 — 多种部署模式 — 不同基础架构环境可参与同一套 Cyberhood 逻辑架构。
- 逻辑架构与实体拓扑有所区别 — 部署拓扑决定资源在哪里运作；平台架构决定企业能力如何与这些资源形成关系。
- 原生分散式设计 — 运算、储存、网路、节点、服务、受保护资讯与组织据点，可依部署需求参与分散式架构。
- 共同架构不要求站点完全相同 — 不同组织据点可采用不同的基础架构与服务责任。
- 集中协调不等于完全中央集中 — 分散式据点可参与整体平台，而不必将架构简化为仅远端存取单一中央系统。
- 服务配置与受保护资讯配置有所区别 — 平台或应用服务的运作位置，本身不会定义其完整受保护资讯的所在位置。
- 高可用性与复原服务不同目标 — 高可用性著重维持服务持续性；复原导向架构著重恢复服务。
- 安全延伸至各种部署模式 — 身分、验证、授权、安全通讯、主机防护、恶意程式防护与资讯保护，在不同部署拓扑中仍持续适用。
- 协作不受实体站点位置限制 — 组织工作空间与协作服务是在站点拓扑之上的逻辑企业环境。
- 应用运作于基础架构拓扑之上 — 业务应用责任与对单一固定实体基础架构位置的依赖彼此分离。
- 模组化扩充是多维度的 — 运算、节点、储存、站点、应用与平台容量可依组织需求演进。
- 部署特性取决于实际设定 — 可用性、复原、效能、安全设定与服务行为，取决于参与的基础架构、服务、应用与部署设计。

重点摘要

- Cyberhood 不要求单一固定的实体部署拓扑。
- 私有企业、私有云、混合云、多站点企业、分散式本地节点与复原导向部署，均可在更广泛的 Cyberhood 架构中运作。
- 平台架构与实体部署拓扑彼此相关，但仍属不同的架构责任。
- 站点拓扑、服务拓扑与受保护资讯拓扑，代表不同的架构责任。
- 高可用性提供服务持续性的架构基础；复原导向架构则处理服务恢复。
- Cyberhood SPAN 在参与的储存资源之间提供 Protected Information Layer，但不表示服务配置与资讯配置必然相同。
- 安全、协作、企业应用与应用扩充能力，在不同部署模式下仍与共同平台架构保持连结。
- Cyberhood 部署架构可随基础架构与组织需求变化而模组化演进。

一套平台架构 — 多种部署模式。

摘要

Cyberhood 的部署模式与参考架构，定义分散式企业平台如何在不同企业基础架构环境中运作，而不需要采用单一强制性的实体拓扑。

此架构将企业服务、共同平台能力、分散式基础架构与受保护资讯区分为彼此相关的架构责任。私有企业、私有云、混合云、多站点企业、分散式本地节点与复原导向部署，提供依组织需求套用此架构的不同方式。

部署架构中特别重要的三个维度为：站点拓扑定义基础架构资源存在的位置；服务拓扑定义平台与应用责任运作的位置；受保护资讯拓扑定义受保护企业资讯如何分散。三者彼此相关，但不能互相等同。

应用在某一站点运作，不代表其完整受保护资讯必然位于该站点。分散式受保护资讯不代表应用一定分散执行；地理基础架构分布也不代表自动 Active-Active 运作或自动地理容错移转。

Cyberhood 高可用性架构透过分散式资源、故障侦测、隔离、重新分配与复原，提供维持服务持续性的架构基础。复原导向部署则处理当中断超过现行环境持续能力后，恢复服务与资讯的不同需求。平台架构本身不定义通用的 RPO、RTO 或自动灾难复原政策。

Cyberhood SPAN 透过 Protected Information Layer 延伸部署架构，使逻辑企业资讯可与分散式受保护储存资源形成关系。安全则持续透过身分、验证、授权、安全通讯、主机防护、恶意程式防护与受保护资讯，作为跨层架构责任运作。

企业协作与企业应用运作于分散式平台基础之上；Cyberhood SDK 与 Distributed Application Framework 则提供额外应用能力参与同一整体架构的路径。

此架构可透过增加运算资源、分散式节点、储存容量、组织站点与应用能力持续演进，而不需要在概念上替换基本平台模型。

企业需求 → 部署模式 → Cyberhood 平台架构 → 站点 + 服务 + 受保护资讯拓扑 → 分散式基础架构资源 → 企业营运能力

一套平台架构 — 多种部署模式。

部署改变架构运作的位置，而不是架构的本质。

Cyberhood — 一套平台架构。多种部署模式。为分散式企业营运而打造。

第 10 章

商业价值与企业优势

执行概述

当基础架构、资讯、应用、安全与组织流程不再是孤立技术领域，而是在协调一致的环境中运作时，企业科技才能形成可持续价值。企业成长过程中，储存、通讯、协作、Workflow、CRM、ERP、安全与开发系统逐步增加，虽各自解决合理需求，却可能造成身分、管理、资讯、安全、基础架构及营运流程碎片化。

Cyberhood 从企业平台架构角度处理此问题，将分散式基础架构、共同平台服务、身分与授权、企业安全、受保护资讯、协作、企业应用及应用扩充整合于共同架构环境。其价值因此超越单一产品功能。

架构 → 平台能力 → 营运能力 → 组织价值 → 企业优势

分散式基础架构为组织延伸、服务持续性与基础架构演进提供基础；共同平台服务在各企业能力之间建立架构一致性；身分与授权则连结人员、组织角色、应用、资讯与受保护资源。

Cyberhood SPAN 提供分散式 Protected Information Layer，旨在降低企业资讯对单一储存资源的不必要依赖，并支援资讯保护、容错、重建及保护状态复原。

协作服务连结人员、通讯、工作空间、企业资讯与组织活动。企业应用则透过 Workflow、Project Management、CRM、ERP 与相关能力支援专业化的业务责任。

Cyberhood SDK 与 Distributed Application Framework 提供可扩充的基础，使其他应用能力能在共同平台架构中持续开发。

这些能力共同建立一套企业平台，不仅支援目前营运，也提供可随组织成长、基础架构变化及未来应用需求持续演进的架构基础。

架构创造能力。能力支援营运。营运创造商业价值。

10.1 从技术架构到企业价值

技术架构本身不会直接创造企业价值；

当架构能力改善组织营运、资讯保护、人员与流程协调、变更管理及未来需求支援能力时，价值才会形成。

Cyberhood 透过结构化的企业价值进程连结这些关系。

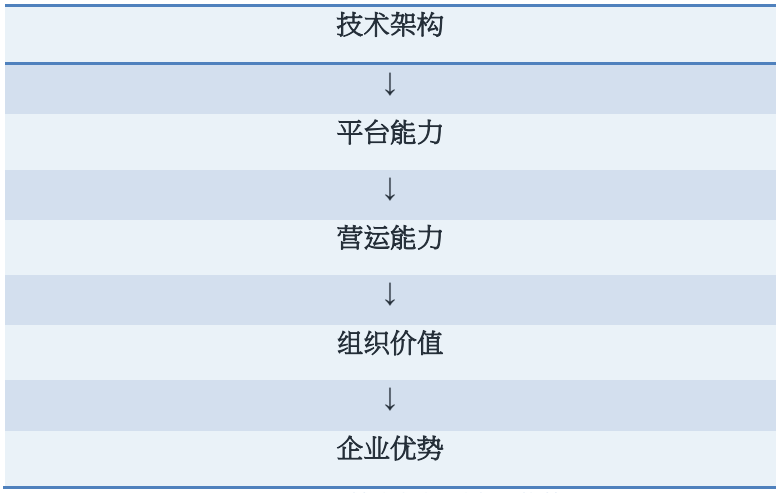


图 10-1 — 从技术架构到企业优势

技术架构提供分散式基础架构、平台服务、身分、安全、受保护资讯、协作、企业应用与 Developer Framework。

平台能力将这些基础转化为可重用的身分验证、授权、资讯保护、协作、Workflow、Messaging、分散式服务与应用整合能力。

营运能力使组织能存取资讯、协调工作、支援分散式使用者、执行业务流程、保护资讯并运作应用。

当这些能力支援一致性、韧性、资讯可用性、协作、治理、适应性与组织协调时，便形成组织价值。

企业优势代表多项企业能力在共同架构基础上运作所形成的长期架构效益。

分散式基础架构 → 分散式营运 → 组织延伸

高可用性架构 → 服务持续性 → 营运韧性

Cyberhood SPAN → 受保护资讯 → 资讯韧性

共同身分与授权 → 一致的存取控制 → 企业治理

协作服务 → 连结人员与资讯 → 组织协调

共同平台 + SDK → 应用扩充性 → 架构演进

科技在架构能力转化为组织能力时，才具有策略价值。

10.2 降低企业科技碎片化

企业科技通常随需求逐步增加，最终可能形成彼此分离的通讯、档案管理、Workflow、Project Management、CRM、ERP、储存、安全、管理与应用开发环境。问题不一定是功能不足，而是独立系统在身分、授权、资讯库、管理、安全控制、基础架构与应用整合上产生不必要重复。

更多系统 → 更多独立基础 → 更高的整合与管理复杂度

Cyberhood 透过共同的分散式企业平台处理此挑战，使多种企业能力能与共享平台服务形成关系。

不同应用仍持续承担不同的业务责任。目标不是让所有应用相同，而是降低在身分、资讯、管理、安全与基础架构上的不必要重复。

业务责任各自专业化；平台服务共享。

目标不是消除专业化，而是降低不必要的架构碎片化。

10.3 统一企业平台

Cyberhood 被设计为统一企业平台，而非互不相关的基础架构与应用产品集合。平台连结分散式基础架构、共同平台服务、身分与授权、企业安全、受保护资讯、协作与资讯服务、企业应用及 Developer Platform。

这些领域在功能上仍各自独立：CRM 不等于储存、身分不等于 Workflow、SPAN 不等于 ERP。改变的是它们之间的架构关系。统一架构 ≠ 相同功能。专业化能力 — 共同架构基础。

这些领域在功能上仍彼此不同。CRM 不会变成储存；身分不会变成 Workflow；Cyberhood SPAN 也不会变成 ERP。改变的是它们之间的架构关系。

统一架构 ≠ 相同功能

统一平台并非要求所有功能都承担相同的责任。它提供了一个通用基础，使各项专业职责能够以一致的方式互动。

身分验证可以作为平台功能运行，而不仅仅是应用程式的特定功能。资讯保护可以作为架构层运行，而不仅仅是孤立的储存功能。协作可以与企业资讯协同运行，而不是作为独立的通讯环境。应用程式可以运行在通用平台服务之上，而无需为每个新的业务功能建立完全独立的架构基础。

专业化能力 — 共同架构基础

10.4 架构整合与一致性

当每个业务能力都引入独立架构基础时，企业科技会愈来愈难协调。

Cyberhood 提供替代模型，使多种企业能力可运作于共享分散式基础架构与共同平台服务之上。

独立基础	共同平台
应用 A → 独立身分	应用 A · B · C
应用 B → 独立授权	共同平台服务
应用 C → 独立基础架构	分散式基础架构
重复管理	协调一致的架构关系

图 10-2 —从独立基础到共同平台

独立应用基础 → 共享平台关系 → 更高的架构一致性

架构整合不要求每个工作负载使用相同实体资源。专业系统、特殊基础架构需求、安全设定与应用责任仍可存在。

目标是降低架构基础上的不必要重复。随需求演进，新增资源与能力可加入既有平台，而不是自动形成另一个孤立环境。

这可提升身分、授权、资讯保护、管理、协作及应用整合的一致性。

较少的独立基础 — 更高的架构一致性

平台整合不等于功能中央集中。

10.5 业务持续性与营运韧性

现代企业营运依赖数位服务、应用与资讯的持续可用。Cyberhood 透过第 3 章的高可用性架构，结合分散式资源、故障侦测、资源隔离、服务或工作负载重新分配、复原及容量恢复，降低单一元件故障直接造成企业营运中断的依赖。

从企业角度而言，价值不只是存在备援资源，而是降低单一故障条件对营运的影响。

分散式资源 → 降低依赖 → 服务持续能力 → 营运韧性

高可用性 → 持续营运

复原导向架构 → 恢复营运

业务持续性是服务持续架构所形成的组织成果。

然而，实际持续与复原特性取决于参与服务、部署拓扑、基础架构设定、资讯架构及组织复原规划。

分散式架构提供韧性基础；实际韧性取决于部署设计。

10.6 将资讯保护视为业务保护

企业资讯不是单纯储存资料；文件、专案资讯、客户纪录、财务资讯、营运资料、组织知识与流程纪录直接参与企业活动。资讯不可用、遭入侵、损毁或无法存取，会影响业务流程、客户关系、组织协调、财务营运与服务持续性。因此，资讯保护应被理解为企业的责任，而不仅仅是储存的责任。

Cyberhood 将身分、验证、授权、安全通讯、主机保护、恶意程式防护及 Cyberhood SPAN 连结为分层资讯保护架构。

资讯保护 → 营运保护 → 业务保护

Cyberhood SPAN 透过将逻辑企业资讯与对单一储存资源的不必要依赖分离，从而发挥其作用。 SPAN 透过受保护的分段、加密、分散式部署、容错、重建、资源隔离和保护状态复原，在企业资讯服务之下提供受保护的资讯层。在受保护储存之前进行恶意程式侦测，为资讯生命周期增添了额外的保护阶段。该架构并非旨在消除所有资讯风险。相反，它建立了多重保护关系，旨在减少不必要的依赖，并为企业资讯提供多阶段的保护。

保护企业资讯，就是保护依赖该资讯的营运。

资讯韧性是营运韧性的先决条件。

10.7 多站点企业的分散式营运

现代组织通常跨多个实体和基础架构环境运作。总部、分公司、区域设施、营运站点、资料中心、远端位置和外部基础架构都可能参与企业营运。

因此，架构挑战不仅在于如何连接各个位置，更广泛的挑战在于如何在这些位置之间维护一致的企业营运环境。

Cyberhood 透过第 9 章中建立的分散式部署模型来满足这项需求。组织内的各个站点可以在通用平台架构中参与，同时保留符合本地需求的基础架构和服务职责。

分散式本地节点（DLN）提供了一种机制，可以将 Cyberhood 平台的功能扩展到适当的分散式位置。

分散式位置 → 共同平台架构 → 协调一致的企业营运

目标并非使每个站点的架构完全相同。不同的地点可能需要不同的运算、储存、网路、平台服务、应用程式或本地资源组合。其价值在于跨越这些差异，维持架构的共通性。

共同企业架构不要求相同的站点基础架构。

分散式营运不应自动形成分散式科技孤岛。

地理分散 → 平台一致性 → 组织协调 → 企业延伸

10.8 企业协作与组织生产力

企业运作依赖人、沟通、资讯、职责和组织流程之间的关系。当这些要素在一个互联的环境中运作，而不是在孤立的通讯和资讯系统中运作时，协作效率会更高。

Cyberhood 将组织身分与沟通、资讯管理、工作空间、共享、版本控制、搜寻和企业工作协调连结起来。

工作空间包括我的空间、公共空间、我分享的空间与分享给我的空间，代表逻辑资讯环境，而非实体站点位置。

人员 + 通讯 + 资讯 + 协作 → 组织工作

这种架构的价值并非仅仅体现在提供独立的协作功能上。其意义在于将协作置于与身分和授权、企业资讯、受保护资讯、企业应用和分散式基础架构相同的更广泛的平台架构之中。这使得使用者沟通方式、资讯存取和共享方式、组织工作执行方式以及资源保护方式之间实现了连续性。

此架构能够减少沟通、资讯存取、共享、协作和业务流程之间不必要的割裂，进而提升组织效率。然而，最终的效率提升取决于组织流程、使用者采纳率、应用设计、营运实务和部署配置。

协作不只是通讯，而是人员与企业资讯之间的架构关系。

架构基础	营运能力	企业价值
高可用性（HA）	服务持续性	营运韧性
Cyberhood SPAN	受保护资讯	资讯韧性
多站点架构	协调分散据点	企业延伸能力
协作平台	连结人员与资讯	组织协调

图 10-3 — 从平台架构到企业营运

10.9 整合式企业应用

企业营运依赖各种应用程式，这些应用程式负责不同的组织和业务职责。 Cyberhood 的企业应用生态系统涵盖工作流程、专案管理、客户关系管理 (CRM)、企业资源规划 (ERP) 及相关功能。这些应用程式之所以保持专业化，是因为它们所负责的职责本质上各不相同。 Cyberhoodd 的架构价值并非在于试图让这些应用程式完全相同，而是让专业化的应用程式与通用的企业平台基础协同运作。

专业化企业应用 → 共享平台基础 → 整合式企业营运

应用程式可以与身分验证、授权、资讯服务、协作、工作流程机制、受保护资讯、分散式资源和管理等通用功能协同运作。这降低了每个新业务应用程式都需要建立完全独立的架构基础的必要性。

业务责任各自专业化；平台服务共享。

应用整合不等于功能融合。

10.10 共同身分、授权与企业治理

身分不只是登入机制；在企业平台中，它建立人员、组织角色、应用、资讯、权限与企业资源之间的关系。

身分 → 验证 → 授权 → 企业资源

从企业角度而言，此架构为协作、资讯存取、企业应用及分散式应用服务建立治理基础。

身分 → 角色 → 权限 → 资源 → 活动

这提供架构基础，用以判断并决定谁正在与平台互动、其组织角色为何、可存取哪些资源，以及何种活动可以被执行。

仅靠身分和授权并不能建立完整的企业治理或合规架构。治理还取决于组织政策、管理程序、应用程式设计、安全控制和营运监督。然而，共同的身分和授权提供了一个一致的架构基础，使这些治理职责得以有效运作。

共同身分 → 一致授权 → 协调一致的资源治理

身分将组织连结至技术架构。

10.11 企业资讯生命周期价值

企业资讯在其整个生命周期中不断演变。它可以被创建、储存、共享、协作、版本控制、搜寻、重复使用、保护，并融入组织流程中。

建立 → 储存 → 分享 → 协作 → 版本化 → 搜寻 → 保护

资讯只有在以下情况下才能创造组织价值：授权使用者可存取资讯、需要时可寻找资讯、可在协作和应用程式中使用讯息，并受到适当保护。

此生命周期的重要性在于，Cyberhood 不只将企业资讯视为储存装置上的档案，而是视为跨协作、应用、安全与组织流程参与的企业资源。

人员 + 协作 + 应用 + 安全 + 组织流程

资讯 → 可存取性 → 协作 → 重复使用 → 保护 → 组织知识

储存保存资讯；资讯生命周期则从资讯创造组织价值。

企业资讯的价值不只取决于其存在，也取决于可用性、可发现性、授权使用与保护。

资讯生命周期管理与资讯保护是互补责任。

10.12 安全、治理与架构一致性

当身分、授权、安全、资讯、基础架构与管理分散于许多互不相关的环境时，企业科技复杂度会提高。更大的问题不是系统数量，而是组织必须协调多少独立架构关系。

Cyberhood 透过共同平台架构，使身分验证、授权、资讯服务、分散式储存、Workflow、Messaging、SDK 服务、管理、安全与受保护资讯彼此形成关系。安全跨越身分、验证、授权、安全通讯、主机保护、恶意程式防护及受保护资讯等多层。

较少的独立基础 → 更高的平台一致性 → 更协调的治理

安全运作跨越多个层面，包括身分识别、身分验证、授权、安全通讯、主机保护、恶意程式防护和资讯保护。

通用平台架构的目的并非在于让企业 IT 维运变得简单。分散式企业环境依然复杂，需要相应的规划、架构、管理、配置、监控、维护和安全策略。

其价值在于架构的一致性。

架构一致性可降低独立技术基础之间不必要的协调成本。

营运简单化不是目标；协调一致的架构才是。

10.13 模组化成长与架构投资保护

企业技术需求不断演变。组织可能会增加使用者、应用程式、运算资源、储存容量、分散式节点、业务功能和组织站点。

Cyberhood 透过模组化分散式架构来应对这种演进。成长可以发生在运算、分散式节点、储存、站点、平台容量和应用程式等各个方面。这些维度无需按特定顺序扩展。

组织可以在不新建站点的情况下增加储存容量，在不取代整个基础架构的情况下引入新应用程式，或根据营运需求将平台扩展到新的组织位置。

模组化扩充 → 架构连续性 → 降低根本性平台替换需求

架构投资保护并不意味著基础架构永远不需要更换，技术永远不会过时，或扩展无需额外成本。它的意义是，即使基础架构、应用程式和组织需求不断演变，通用平台模型也能保持其效能。

投资保护更应理解为架构连续性，而非技术永久性。

10.14 支援组织成长

组织的发展会从根本上改变技术需求，而这种改变远不止于基础架构的承载能力。企业可能会增加员工、设立部门、开设分支机构、引入新的业务流程、增加资讯量、部署更多应用程式，或扩展到地理分散式营运。

Cyberhood 的设计旨在使这些变化能够在更广泛的分散式平台模型中持续进行。

初始组织 → 增加人员 → 增加流程 → 增加应用 → 增加站点 → 增加企业复杂度

在这演变过程中，分散式基础架构、通用平台服务、资讯、协作、企业应用和业务营运之间的基本关系始终至关重要。因此，其价值远不止于硬体可扩展性。

组织成长不需要在每个阶段都重新建立企业架构概念。

组织成长应扩展平台，而不是碎片化架构。

10.15 应用扩充性与未来需求

企业需求并非一成不变。随著组织的演进，新的流程、服务、整合、资讯流和应用需求不断涌现。

Cyberhood SDK 和分散式应用程式框架提供了一个架构基础，在此基础上，可以基于通用平台开发额外的应用功能。

目前应用 + 未来应用 → 共同平台基础

根据应用程式设计，新应用程式可以与身分验证、授权、分散式服务、资讯、工作流程、讯息传递、受保护资源和管理等通用功能协同运作。因此，该平台在概念上并不局限于某一特定时间点可用的应用程式。然而，可扩展性并不意味著未来的所有应用程式需求都会自动被满足。其价值在于提供一个基础，在此基础上可以开发额外的应用程式功能。

扩充性不是预测未来需求，而是提供回应未来需求的架构。

10.16 降低应用与基础架构孤岛

企业软体中功能专业化不可或缺。 CRM 和 ERP 分别负责不同的业务职责。工作流程管理和专案管理支援不同的组织流程。协作管理和资讯管理满足不同的使用者和资讯需求。

当功能专业化自动造成平台隔离和基础架构孤岛时，就会出现架构问题。 Cyberhood 将这些概念分离出来。应用程式可以在保留其专业业务职责的同时，根据需要参与到与身分、授权、资讯、工作流程、讯息传递、储存、管理、受保护资讯和分散式基础架构的通用关系中。

专业化应存在于业务层，而不必在每一技术层都形成架构隔离。

业务责任各自专业化；平台服务共享。

这可降低每个新应用都必须建立完全独立技术基础的架构压力。

10.17 管理可视性与营运监督

企业治理不仅需要制定资源存取规则，还需要对企业服务的使用进行管理可见性。

Cyberhood 提供包括组织身分、授权、资源权限、管理和活动记录在内的架构元素，这些元素有助于实现营运监督。

身分 → 角色 → 权限 → 资源 → 活动

在此模型中，活动资讯可以支援管理监督、营运审查和组织监管。这些功能不应被解读为构成适用于所有产业的完整监管合规、审计或治理架构。它们提供的是平台级机制，组织可以将其融入更广泛的治理和管理实践中。

治理规则 → 授权活动 → 管理可视性

治理定义关系；可视性协助组织观察其实际运作。

10.18 长期架构弹性

企业科技决策具有长期影响：基础架构改变、组织扩张、应用演进、资讯量增加、安全需求发展、新流程出现。Cyberhood 透过架构责任分离处理此挑战。

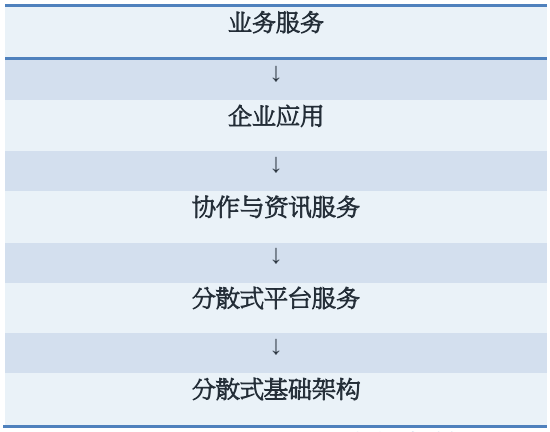


图 10-4 — Cyberhood 分层架构连续性

这种分层模型并非意味著每一层都可独立更改而无需整合或维运工作。相反，它建立了架构职责之间的概念分离。

可以引入额外的基础架构。可以开发新的应用程式。可以加入新的组织站点。资讯和协作服务可以在更广泛的平台模型中继续运作。

架构演进应延伸平台，而不是不必要地取代其基本关系。

技术会改变；架构关系提供连续性。

10.19 Cyberhood 企业价值模型

Cyberhood 的企业价值不是来自单一能力，而是来自各架构层之间的协调关系。

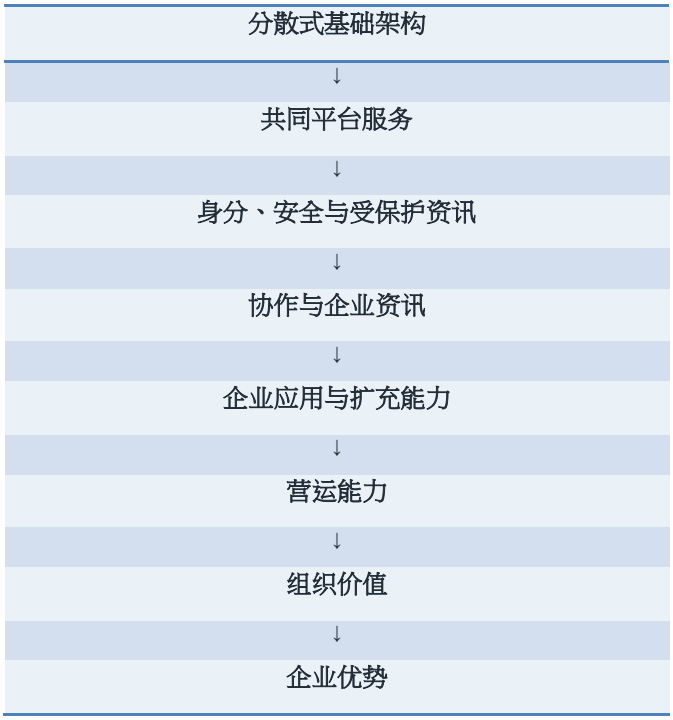


图 10-5 — Cyberhood 企业价值模型

分散式基础架构提供技术基础。通用平台服务建立身分、授权、资讯、通讯、管理、工作流程和分散式服务之间的共享关系。

安全性和 Cyberhood SPAN 保护企业使用者、服务、资源和资讯之间的关系。协作和资讯服务将人员与组织资讯和工作连结起来。

企业应用程式将通用平台功能转化为专门的业务流程。 Cyberhood SDK 扩展了此架构，使其能够支援未来的应用程式功能。

这些架构元素构成了营运能力。当平台支援连续性、资讯韧性、协作、治理、分散式营运和组织发展时，营运能力就能创造组织价值。

架构 → 能力 → 营运 → 组织价值 → 企业优势

Cyberhood 的价值不是由单一能力定义，而是由连结这些能力的架构定义。

10.20 策略性企业优势

Cyberhood 分散式企业平台建立一组源自各架构层相互关系的策略性企业优势。

- 统一企业架构 — 基础架构、平台服务、资讯、安全、协作、应用与扩充性在协调一致的框架中共同参与。
- 分散式企业营运 — 总部、分公司、区域设施及其他参与环境可在共同的分散式平台模型中运作。
- 资讯韧性 — 多层安全控制与 Cyberhood SPAN Protected Information Layer 形成关系。
- 营运韧性 — 分散式基础架构与高可用性为服务持续性提供基础，而复原导向架构则支援服务恢复。
- 整合式协作 — 人员、通讯、资讯、分享、工作空间、搜寻与组织工作在共同平台中形成关系。
- 整合式企业应用 — Workflow、Project Management、CRM、ERP 与相关应用保留专业业务责任，同时共享共同平台能力。
- 应用扩充性 — Cyberhood SDK 与 Distributed Application Framework 为其他应用开发提供架构基础。
- 模组化演进 — 运算、储存、节点、站点及应用能力可依组织需求持续演进。
- 长期架构一致性 — 随组织演进，基础架构、平台服务、资讯、应用与业务营运之间的基本关系仍可持续有效。

因此，Cyberhood 的定位不只是技术集合，而是分散式企业营运与长期组织演进的架构基础。

关键架构原则

- 架构优先于碎片化 — 企业能力应在协调一致的架构关系中运作，而不是每次新增能力就自动引入独立技术基础。
- 共享平台基础 — 身分、授权、资讯、通讯、管理、受保护资源及分散式基础架构提供可重用的平台能力。
- 业务责任各自专业化；平台服务共享 — 应用保留专业化业务责任，同时参与共同平台基础。
- 企业应用整合 — API Integration、Transaction Orchestration、ESB、Message Bus、Automatic Cross-Application Synchronization 与共享工作流程连接专业化应用，而不要求功能趋同。
- 资讯作为企业资产 — 企业资讯参与协作、应用、搜寻、安全、治理与业务流程。
- 原生分散式设计 — 企业资源与组织站点可参与更广泛的分散式架构。
- 以架构实现安全与治理 — 身分、授权、安全通讯、主机保护、受保护资讯、资源权限与管理可视性作为彼此相关的架构责任运作。
- 以架构支援持续性 — 分散式资源、高可用性机制与复原导向架构为服务持续与恢复提供基础。
- 扩充性作为平台能力 — Cyberhood SDK 使平台架构能超越固定的应用集合持续扩充。
- 模组化演进 — 基础架构、储存、站点、应用与平台容量可依组织需求演进。
- 长期架构一致性 — 企业可持续成长，同时维持基础架构、平台服务、资讯、应用与业务能力之间的基本关系。

企业重点摘要

- Cyberhood 将分散式技术架构与企业营运能力连结。
- 共同平台架构可降低基础架构、资讯、安全、协作与应用之间不必要的碎片化。
- 高可用性与复原导向架构分别为服务持续与恢复提供互补的架构基础。
- Cyberhood SPAN 将受保护资讯定位为整体企业架构的一部分，而不是孤立的储存功能。
- 共同身分与授权为一致的资源治理提供基础。
- 协作连结人员、通讯、企业资讯与组织工作。
- 专业化企业应用可保留其业务责任，同时共享共同平台服务。
- Cyberhood SDK 与模组化架构为组织及应用演进提供基础。
- Cyberhood 的策略价值来自分散式基础架构、受保护资讯、协作、企业应用、治理与扩充性之间协调一致的关系。

架构创造能力。能力支援营运。营运创造商业价值。

摘要

Cyberhood 分散式企业平台的商业价值，来自基础架构、平台服务、受保护资讯、协作、企业应用、安全、治理与应用扩充性之间协调一致的关系。

分散式基础架构为不同位置与部署环境提供技术基础；共同平台服务则在身分、授权、资讯、通讯、管理、Workflow、储存、应用及分散式资源之间建立一致的关系。

Cyberhood 高可用性架构为服务持续性提供基础，而复原导向架构则处理较重大中断后的服务恢复。

Cyberhood SPAN 透过分散式分段、加密、配置、设定式容错、重建与保护状态复原，提供 Protected Information Layer。

企业协作连结人员与通讯、工作空间、资讯分享、搜寻及组织活动；Workflow、Project Management、CRM、ERP 与相关企业应用则将平台能力转化为专业化组织流程。

身分与授权连结人员及组织角色与企业资源；管理可视性与活动纪录则可支援治理与营运监督。

Cyberhood SDK 与 Distributed Application Framework 使架构超越固定的应用集合，并为其他应用开发提供基础。

模组化扩充使运算资源、储存资源、分散式节点、组织站点及应用能力可随需求变化而演进。

分散式基础架构 → 共同平台服务 → 安全与受保护资讯 → 企业整合服务 → 协作与企业资讯 → 整合式企业应用 → 协调式企业流程 → 业务营运

目标不只是提供更多科技，而是建立一套架构基础，使企业科技在基础架构、资讯、应用、安全需求与组织营运持续演进时，仍能维持协调一致。

架构创造能力。能力支援营运。营运创造商业价值。

Cyberhood — 从分散式架构到可持续的企业能力。

企业应用整合作为组织价值

企业应用整合的价值，在于连接专业化业务责任，而不要求功能趋同。ERP、CRM、EIP、专案管理、工作流程／电子签核、通讯与协作及其他应用，可依各自业务角色持续演进，同时参与协调一致的企业流程。

API 整合连接应用功能与资讯；交易编排协调跨越应用边界的活动；工作流程整合组织程序；讯息与服务整合连接参与系统；跨应用自动同步维持相关资讯与流程状态关系。这些能力共同支援组织协调与营运可视性。

因此，平台整合不代表功能集中化。Cyberhood 透过共同的整合与平台关系，降低架构碎片化，同时保留专业化应用的责任。

应用整合 → 交易编排 → 流程整合 → 资讯同步 → 组织协调 → 营运可视性 → 企业治理

应用整合不等于功能趋同。

平台整合不等于功能集中化。

第 11 章

结论与架构愿景

执行概述

企业科技持续在基础架构、资讯、安全、协作、应用与组织营运等面向演进。

随著新需求出现，企业经常透过新增系统、新增基础架构、新增安全机制、新增资讯储存环境与新增应用来因应。每一项新增项目都可能解决当下需求，但长期下来，组织可能日益依赖一组彼此独立设计的科技环境。

Cyberhood 提出不同的架构方法。

Cyberhood 分散式企业平台的设计原则，是让企业科技以协调一致的架构运作，而不是持续累积彼此孤立的系统。

其架构连结分散式基础架构、共用平台服务、身分与授权、企业安全、受保护资讯、协作与资讯服务、企业应用，以及可扩充的 Developer Platform。

这些能力在功能上仍各自专业化，但共同参与于同一个架构环境。

因此，Cyberhood 的重要性不仅在于个别技术所提供的能力，更在于这些技术之间所建立的关系。

基础架构 → 平台服务 → 企业能力 → 业务营运

Cyberhood 将此关系延伸至分散式组织环境，同时让身分、资讯、安全、协作、应用与平台服务维持为彼此相关的架构责任。

Cyberhood 并非由其所包含的技术来定义，而是由连结这些技术的架构所定义。

由此形成的愿景，是一个既能支援目前组织需求，又能为持续演进提供架构基础的企业平台。

11.1 从个别系统到分散式企业平台

企业科技环境很少一开始就是统一架构，而是随时间逐步演进。

组织导入储存系统管理资讯、通讯系统连结使用者、工作流程应用协调流程、CRM 管理客户关系、ERP 支援企业营运、安全技术保护资源，以及基础架构平台支援应用。

每项技术都有其合理责任。当每一项新责任都导入另一套独立基础时，架构挑战便随之产生。

因此，功能成长长期可能转化为架构碎片化。

Cyberhood 从相反方向思考企业科技。它不是先从个别产品出发，再尝试事后整合，而是先建立分散式平台架构，让不同企业能力在其中参与。

这并不表示所有企业能力都变成同一个应用。Workflow 仍是 Workflow，CRM 仍是 CRM，ERP 仍是 ERP，协作仍是协作；安全与受保护资讯也仍是不同的架构责任。

改变的是这些能力参与企业环境时所依循的架构基础。

目标不是消除专业化技术，而是避免专业化自动演变成架构孤岛。

新需求 → 新系统 → 新基础架构 → 新身分体系 → 新资讯环境 → 新管理责任

个别系统 → 共用平台关系 → 分散式企业平台

平台优先于产品

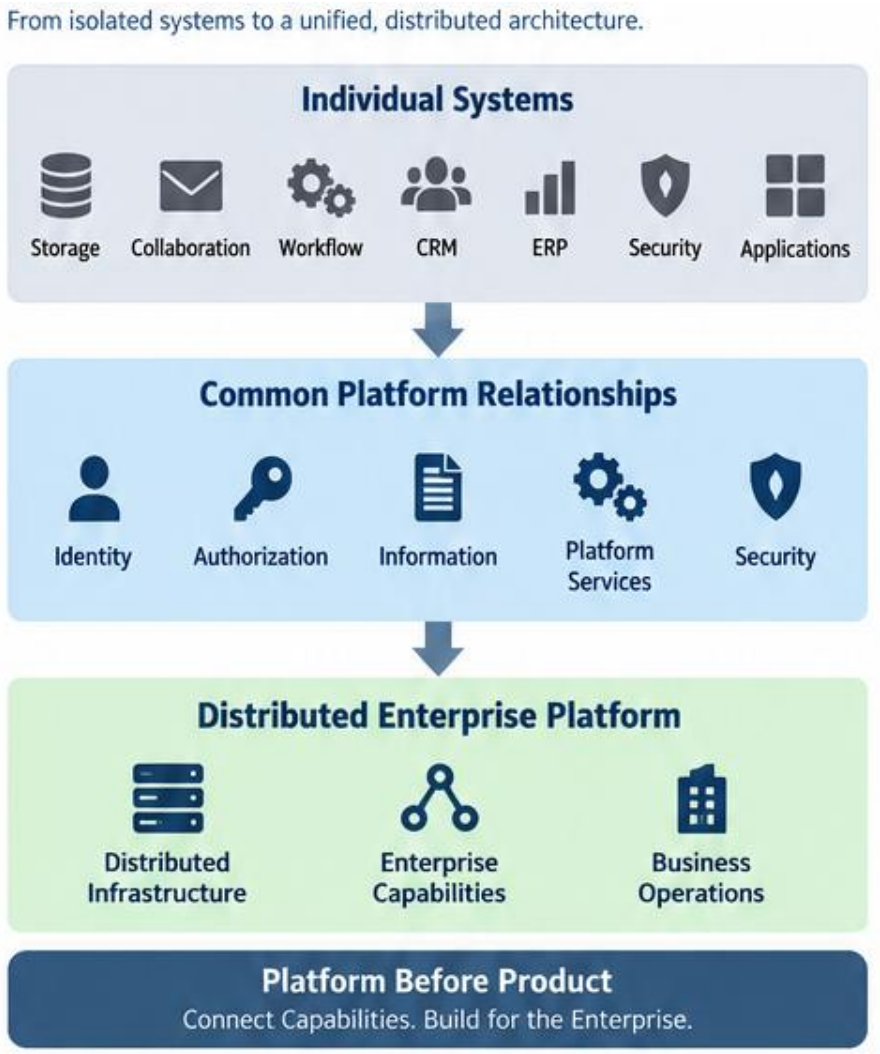


图 11-1 — 从个别系统到分散式企业平台

11.2 统一的架构基础

统一企业平台并不要求每一项科技能力执行相同功能，而是要求不同能力在明确定义的架构关系中运作。

Cyberhood 透过分层式企业架构建立这些关系。

分散式基础架构提供平台所需的运算、储存、网路、分散式节点及其他参与式基础架构资源。

分散式平台服务提供共用架构能力，使较高层级的企业服务可与分散式资源建立运作关系。

协作与资讯服务将组织使用者与通讯、工作空间、资讯分享、版本管理、搜寻及受保护资讯服务连结。

企业应用将平台能力转化为专业化组织功能，例如 Workflow、Project Management、CRM、ERP 及相关企业应用。

业务服务代表最终由科技架构所支援的组织活动与责任。

各层在维持架构关系的同时建立责任分离。业务应用可保持专业化并使用共用平台能力；资讯可跨协作与应用参与，同时持续与授权及保护机制相连；基础架构可持续演进，而较高层级的架构责任仍维持概念一致性。

统一架构不应与单体式架构混为一谈。Cyberhood 统一的是架构关系，同时保留分散式资源、专业化责任与模组化部署。

业务服务 → 企业应用 → 协作与资讯服务 → 分散式平台服务 → 分散式基础架构

责任分离不代表架构必须分离。

不同责任 — 共同架构基础

统一架构 ≠ 单体式架构

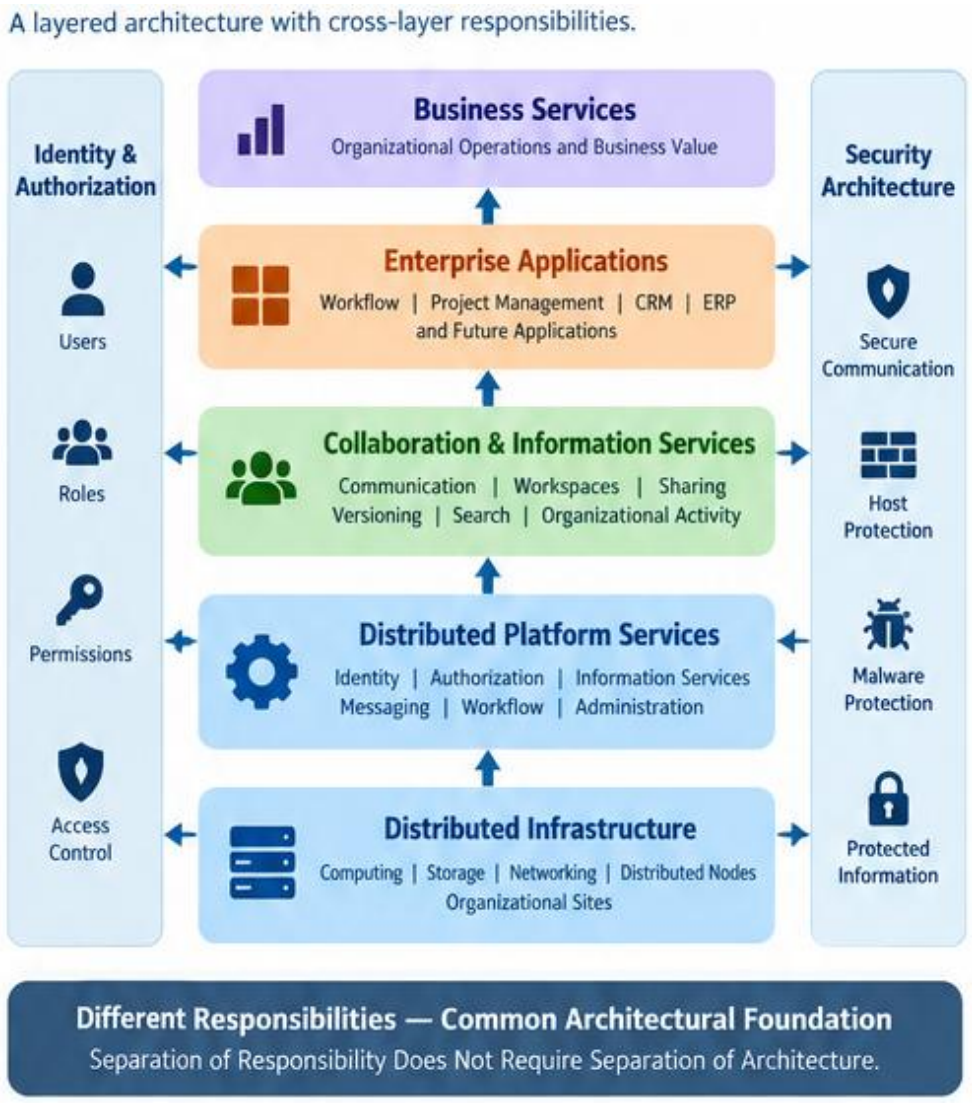


图 11-2 — Cyberhood 统一架构基础

11.3 原生分散式设计

Cyberhood 的分散式概念并不限于伺服器的实体配置，而是一项更广泛的架构特性。

企业使用者、组织站点、运算资源、储存资源、应用、服务与受保护资讯，都可跨不同基础架构环境参与。

因此，Cyberhood 将分散式视为平台架构的一部分，而不是平台完成后才额外加入的例外机制。

此分散式模型涵盖 Master Node、Slave Node、分散式本地节点（Distributed Local Node, DLN）、运算资源、储存资源、网路资源与组织站点之间的关系。这些资源可依部署需求参与更广泛的 Cyberhood 环境。

分散式是为企业韧性、多站点营运、资源参与、受保护资讯配置与模组化成长提供架构基础。

Cyberhood 不假设每一项企业能力都必须依赖单一伺服器、单一储存装置或单一组织位置。

同时，分散式也不应被解读为自动高可用性、自动地理容错移转或全面复写。实际的服务持续性、服务配置、受保护资讯配置与复原行为，取决于架构与部署设定。

企业分散式架构也存在于多个面向。基础架构拓朴、服务拓朴、受保护资讯拓朴与组织站点拓朴彼此相关，但在架构上各自独立。

分散式资源 → 降低依赖

分散式节点 → 跨基础架构的服务参与

分散式站点 → 多站点企业营运

分散式受保护资讯 → 资讯韧性

模组化资源 → 架构演进

原生分散式设计

分散式架构创造架构上的可能性；部署设计决定实际营运行为。

11.4 资讯作为企业资产

企业资讯是组织中最具持续性的资源之一。基础架构可以更换、应用可以演进、装置可以改变、组织结构可以重整，但企业资讯往往会跨越这些变化持续存在。

文件、客户纪录、专案资讯、营运资料、财务资讯、流程纪录、通讯内容与组织知识，不只是被储存的档案，而是直接参与企业营运。

因此，Cyberhood 将资讯视为企业资产，而不只是存在于储存装置上的资料。在整个生命周期中，企业资讯会与身分、授权、协作、应用、安全及受保护储存互动。Cyberhood SPAN 进一步将逻辑受保护资讯与对个别储存资源的不必要依赖分离。因此，不应只透过受保护元件所在的实体装置来理解一个逻辑企业资讯物件。

逻辑企业资讯不应仅由实体拓朴所定义。资讯保护同时包含两种彼此相关但不同的关系。存取控制关系处理谁可以存取企业资讯；受保护资讯关系则处理受保护资讯如何跨分散式储存资源运作。

档案储存在哪里？ → 企业资讯如何参与组织运作？

建立 → 储存 → 分享 → 协作 → 版本化 → 搜寻 → 保护

身分 → 授权资讯存取 → 协作 → 应用 → 组织知识

资讯是逻辑企业资源；储存是基础架构资源。

储存位置 ≠ 资讯身分

应用位置 ≠ 完整资讯位置

使用者位置 ≠ 资讯位置

身分 → 验证 → 授权 → 受保护资讯

分段 → 加密 → 分散 → 重建 → 复原

资讯保护同时是存取控制责任，也是资讯架构责任。

11.5 安全即架构

企业安全不能被简化为单一产品、装置、网路边界或控制点。

使用者存取应用，应用存取资讯，资讯跨网路移动，基础架构承载服务，组织角色建立责任；每一种关系都会产生安全需求。

因此，Cyberhood 将安全视为跨平台运作的架构责任。

身分建立谁正在与企业环境互动；验证确认该身分是否可被验证；授权依组织角色与权限决定可使用的资源与动作；受保护资源则代表由这些关系所治理的资讯、应用、服务与平台能力。

其他架构保护机制包括安全通讯、针对分散式主机的 Independent Firewall 保护、恶意程式防护，以及 Cyberhood SPAN 受保护分散式资讯储存。

这些机制分别处理不同责任。任何单一机制都不应被解读为可以消除所有安全风险。架构目标是在彼此相关的企业资源与服务之间建立分层保护。

因此，安全是一项跨层责任，而不是独立的应用层。

身分 → 验证 → 授权 → 受保护资源

身分安全 + 通讯安全 + 主机保护 + 资讯保护 → 企业安全架构

安全不是单一边界，而是跨越架构各层的关系。

安全控制保护元件；安全架构保护关系。

11.6 协作作为平台能力

组织透过人员、资讯、通讯、责任与业务流程之间的关系运作。因此，企业协作不能只被视为讯息传递或通讯。

通讯可以启动工作，但企业协作还依赖资讯存取、共享情境、组织角色、应用与业务流程。

因此，Cyberhood 将协作定位为原生平台能力。

Enterprise Mail 与 Enterprise Messenger 支援组织通讯；档案管理、版本控制、全文搜寻、分享与跨平台存取则将使用者与企业资讯连结。

工作空间模型 — 我的空间（My Space）、公共空间（Public Space）、我分享的空间（Sharing With Space）与分享给我的空间（Shared From Space）— 用来组织使用者与组织参与者之间的逻辑资讯关系。

此模型的重要性在于协作并未与更广泛的平台隔离，而是与身分及授权、企业资讯、受保护资讯、企业应用与分散式基础架构建立关系。

人员 + 身分 + 通讯 + 资讯 + 业务流程 → 企业协作

协作是人员与企业资讯之间的平台关系。

通讯连结人员；协作连结人员、资讯与工作。

11.7 应用作为平台的一部分

企业应用承担专业化业务责任。Workflow 支援结构化流程与签核；Project Management 支援专案导向活动；CRM 支援客户关系、服务活动、互动历程及相关资讯；ERP 则支援更广泛的企业营运领域，包括销售、采购、会计、资产、库存、制造、人力资源、预算及相关流程。

这些应用构成 Cyberhood 企业应用生态系统与整合。

然而，Cyberhood 的架构模型并不受限于固定的一组预先定义应用。

Cyberhood SDK 与 Distributed Application Framework 提供基础，使其他应用可在与分散式平台服务及企业资源建立关系的前提下进行开发。

应用仍负责专业化业务逻辑；平台则依应用设计提供共用架构关系，包括身分、授权、资讯服务、协作、分散式服务、受保护资源与基础架构存取。

既有应用 + 未来应用 → 共用分散式平台

应用是专业化业务能力；平台是共享的架构基础。

应用参与平台，但不定义平台。

11.8 一个平台架构 — 多种部署模式

企业组织运作于不同的基础架构条件。有些维持私有控制的基础架构，有些采用私有云环境，有些结合私有与外部基础架构；许多企业则跨总部、分公司、区域设施或其他分散式组织位置营运。以复原为导向的基础架构也可参与更广泛的企业架构。

Cyberhood 不要求这些组织采用完全相同的实体拓朴，而是将逻辑架构与实体部署拓朴分离。

逻辑架构定义基础架构、平台服务、资讯、应用与业务能力之间的关系；实体部署则依组织需求决定参与资源、服务与资讯的配置位置。

本白皮书建立部署模式包括私有企业、私有云、混合云、多站点企业、分散式本地节点（DLN）及复原导向部署。

因此，不同部署模式可套用同一个更广泛的平台架构，而不需要完全相同的基础架构。

基础架构 → 平台服务 → 资讯 → 应用 → 业务能力

一个平台架构 — 多种部署模式

逻辑一致性不要求实体一致。

部署改变架构运作的位置，而不是架构本质。

11.9 业务责任各自专业化；平台服务共享

企业应用应依其所支援的业务责任维持专业化。CRM 应处理客户相关责任；ERP 应处理企业资源与营运责任；Workflow 应处理结构化组织流程；Project Management 应处理专案导向活动；协作服务则应支援组织通讯与资讯关系。

Cyberhood 并不试图消除这些差异，而是透过架构将业务责任与平台责任分离。

业务应用保留专业化功能；平台服务则依需要提供可重复使用的架构能力，例如身分、授权、资讯服务、通讯、工作流程机制、管理、受保护资讯及分散式基础架构服务。

此模型让专业化与架构一致性能够并存，也避免假设每一个专业化应用都必须导入一套完全独立的科技基础。

业务责任各自专业化；平台服务共享。

专业化应用 → 共用平台服务 → 共同分散式基础架构

专业化创造业务价值；共享平台服务维持架构一致性。

平台应标准化共同关系，而不是标准化每一项业务功能。

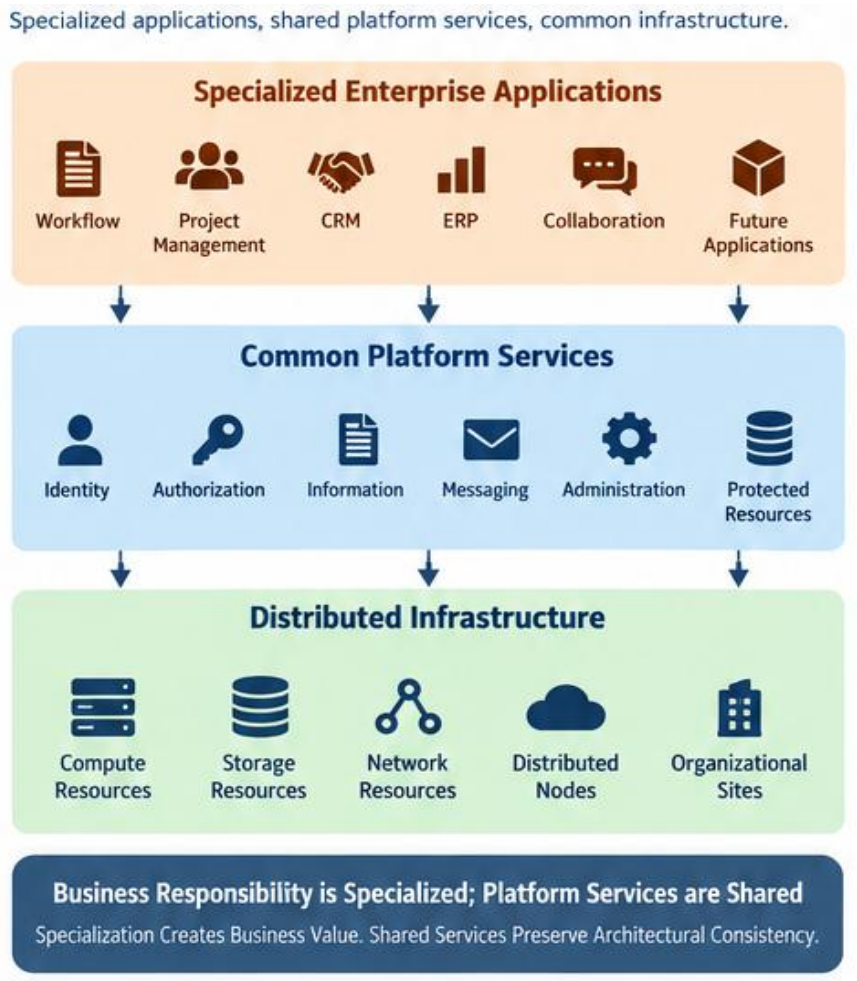


图 11-3 — 共享平台上的专业化企业能力

11.10 持续演进的架构

企业需求持续演进。组织增加使用者、资讯量持续成长、新应用被导入、基础架构容量改变、新增组织据点、安全需求演进，业务流程也持续重新设计。

因此，可持续的企业架构必须支援变化，而不是每当新需求出现时，都要求组织在概念上重新建构整个科技环境。

Cyberhood 透过四项互补的架构特性因应此需求：分层式架构、分散式基础架构、模组化演进与应用扩充性。这些特性共同使平台能跨基础架构、资讯、应用与组织需求持续演进，同时保留共同的概念基础。额外的运算或储存资源可加入分散式环境；分散式本地节点（DLN）可将平台延伸至其他组织位置；企业应用可因应新增或改变的业务流程；Cyberhood SDK 与 Distributed Application Framework 则为其他应用能力提供开发基础。

目标不是科技永久不变。个别产品、基础架构资源与实作细节都会持续改变；架构目标是在变化中维持连续性。

目前需求 → 模组化变更 → 扩充能力 → 持续演进的企业平台

科技会改变，业务需求会演进，架构关系提供连续性。

可持续的架构，是能吸收变化而不失去一致性的架构。

11.11 Cyberhood 架构愿景

Cyberhood 的架构愿景整合了本白皮书所建立的主要关系。

在基础架构层，分散式资源提供技术基础；在平台层，共用服务为身分、授权、资讯、通讯、工作流程、管理、分散式处理与应用参与建立可重复使用的关系。

在协作与资讯层，人员与企业资讯、通讯、工作空间、分享、搜寻及组织活动互动；在应用层，专业化企业系统将平台能力转化为业务流程；在业务层，这些流程支援企业营运。

安全跨越这些层级运作。受保护资讯与身分、授权、协作、应用及分散式储存资源建立关系。部署模式决定架构实际运作的位置，但不重新定义其基本逻辑关系。

因此，Cyberhood 模型的意义并非功能一致化。基础架构仍是基础架构，安全仍是安全，协作仍是协作，应用保留专业化责任，资讯则维持为逻辑企业资源。

Cyberhood 所提供的，是让这些责任能共同参与协调一致企业环境的架构。

分散式基础架构 → 共用平台服务 → 协作与资讯服务 → 企业应用 → 业务服务

一套分散式企业架构，在同一个协调一致的平台环境中连结基础架构、资讯、安全、协作、应用与业务营运。

整合不要求一致化。

协调不要求中央集中。

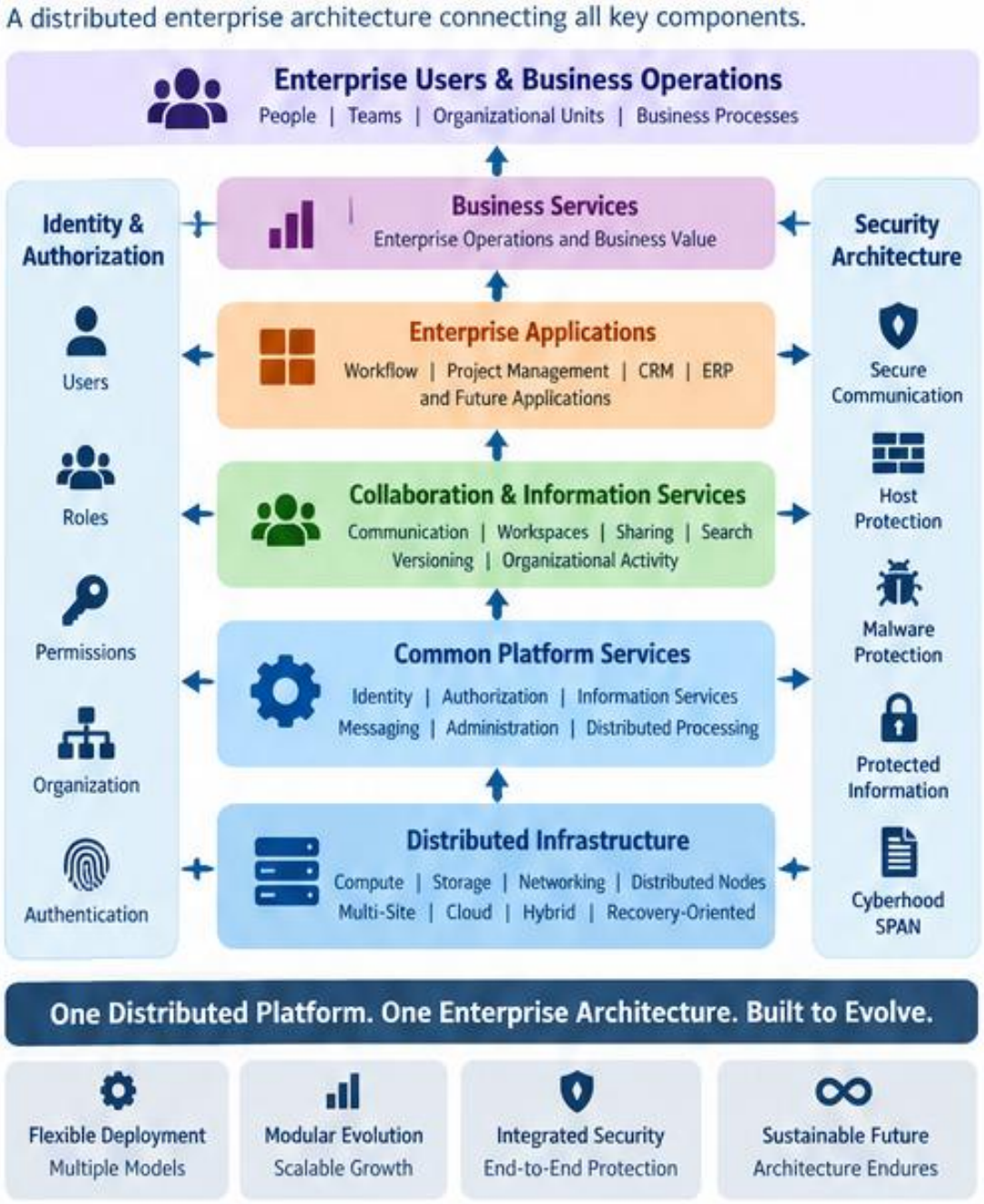


图 11-4 — Cyberhood 架构愿景

11.12 Cyberhood 架构原则

1. 原生分散式设计 — 分散式基础架构是平台基础的一部分，而不是选配延伸。分散式是一项架构特性，而不只是部署选择。

2. 平台优先于产品 — 个别功能与应用参与更广泛的企业平台架构。平台定义关系，产品承担专业化责任。

3. 身分作为基础 — 身分连结使用者、组织角色、授权、应用、资讯与企业资源。身分将组织与科技架构连结。

4. 资讯作为企业资产 — 企业资讯跨储存、协作、搜寻、应用、安全与组织流程参与。资讯是逻辑企业资源；储存是基础架构资源。

5. 安全由架构建立 — 安全跨身分、授权、安全通讯、主机保护、恶意程式防护与受保护资讯运作。安全不是单一边界，而是跨越架构各层的关系。

6. 协作作为原生能力 — 通讯、资讯、分享、工作空间与组织互动共同参与平台。协作连结人员、资讯与工作。

7. 业务责任各自专业化；平台服务共享 — 应用保留专业化业务责任，同时与共用平台能力建立运作关系。专业化与架构一致性可以并存。

8. 一个平台架构 — 多种部署模式 — 不同实体环境可套用同一个更广泛的逻辑平台架构。逻辑一致性不要求实体一致。

9. 模组化演进 — 运算、储存、分散式节点、组织位置与平台容量可随企业需求改变而演进。成长应延伸架构，而不是使架构碎片化。

10. 面向未来开发的扩充性 — Cyberhood SDK 与 Distributed Application Framework 为其他应用能力提供基础。扩充性不是预测未来需求，而是提供回应未来需求的架构。

这些原则共同定义 Cyberhood：它不是固定的科技配置，而是支援分散式企业运算与组织持续演进的架构框架。

最终架构宣言

科技会演进，架构得以延续。

企业科技将持续改变。

基础架构将更加分散，资讯量将持续成长，安全需求将持续演进，组织也会导入新的应用、流程、据点与营运模式。

因此，长期挑战不只是选择个别技术，而是在需求持续演进时，维持一套能将这些技术与企业资讯、人员、应用、安全及组织营运连结的架构。

Cyberhood 并非由任何单一伺服器、储存技术、安全机制、协作工具或企业应用所定义，而是由连结它们的架构所定义。

透过分散式基础架构、共用平台服务、受保护资讯、企业协作、业务应用与可扩充开发框架，Cyberhood 为分散式企业运算建立统一基础。

基础架构 → 平台服务 → 企业能力 → 业务营运

身分 → 验证 → 授权 → 受保护资源

建立 → 储存 → 分享 → 协作 → 版本化 → 搜寻 → 保护

业务责任各自专业化；平台服务共享。

一个平台架构 — 多种部署模式。

目前需求 → 模组化演进 → 未来能力

最终成果不是固定的科技配置，而是一套设计为能与企业共同演进的架构基础。

Cyberhood 并非由其所包含的技术来定义，而是由连结这些技术的架构所定义。

Cyberhood

一个分散式平台。一套企业架构。为持续演进而打造。

架构愿景中的企业应用整合

Cyberhood 企业应用整合将平台愿景从分散式基础架构与受保护资讯延伸至协调一致的企业营运。平台连接专业化应用，而不消除其专业化责任。

分散式架构提供参与基础架构的营运基础；Cyberhood SPAN 为采用 SPAN 保护的资讯提供受保护资讯架构；企业应用整合则连接专业化企业应用之间的 API、交易、讯息、资讯流、工作流程状态与企业流程。

这些能力形成互补的架构关系，不要求所有应用变得相同、所有服务集中化，或所有资讯位于同一实体位置。架构提供共同关系，使专业化能力能在一致的企业环境中运作。

专业化应用 — 整合流程 — 共享平台服务 — 一个企业架构

平台连接专业化应用，而不消除其专业化责任。

一个分散式平台。一套企业架构。为持续演进而打造。

附录 A

技术词汇

本词汇表定义《Cyberhood 分散式企业平台国际白皮书》中使用的主要架构、平台、资讯保护、应用与部署术语。这些定义用以说明各术语在 Cyberhood 架构中的使用方式；若某术语在业界具有更广泛的含义，以下定义则说明其在本白皮书中的特定脉络。

Cyberhood 分散式企业平台

一套分散式企业平台架构，在同一个协调一致的架构环境中，连结分散式基础架构、共用平台服务、身分与授权、企业安全、受保护资讯、协作与资讯服务、企业应用，以及应用扩充能力。

它代表共同的架构基础，使专业化的企业能力得以参与分散式企业营运。

分散式基础架构（Distributed Infrastructure）

由运算、储存、网路、分散式节点及其他参与的基础架构资源所构成，为 Cyberhood 平台跨一个或多个部署环境提供技术基础。

分散式平台服务（Distributed Platform Services）

运作于分散式基础架构之上的共用平台能力，用以支援更高层级的企业服务与应用。这些能力包括身分验证、授权、索引、分散式储存服务、工作流程、讯息传递、SDK 服务、管理，以及本白皮书所述的其他参与式平台服务。

Master Node

Cyberhood 分散式架构中的主要节点角色，依适用的架构与部署设计参与平台协调与服务运作。

Slave Node

参与 Cyberhood 平台的分散式节点角色，依其被指派的架构责任与部署需求提供资源或服务。

分散式本地节点（Distributed Local Node, DLN）

部署于组织或分散式地点的 Cyberhood 节点，用以将平台参与延伸至该环境。分散式本地节点可依部署设计参与被指派的服务、处理、储存或其他平台责任。

分散式本地节点是更广泛 Cyberhood 平台架构的一部分，而非独立运作的平台。

Cyberhood SPAN — Secured & Protected Archive Network

Cyberhood 分散式企业平台的受保护资讯架构。SPAN 透过受保护分段、加密、分散式配置、门槛式重建、装置层级容错与保护状态复原，使逻辑企业资讯降低对个别储存资源的依赖。

SPAN 作为整体 Cyberhood 架构的 Protected Information Layer，并可依平台与部署设计使用参与的储存资源。

Global Index（全域索引）

Cyberhood 平台的索引能力，依平台存取与授权关系，支援跨参与资讯资源的资讯探索与全文搜寻。

高可用性（High Availability, HA）

一种架构方法，透过参与的分散式资源、故障侦测、隔离、重新分配、复原与容量恢复，支援服务持续性。

高可用性主要著重于在适用的故障条件下持续提供服务，不应被视为与灾难复原相同。

灾难复原（Disaster Recovery, DR）

一种以复原为导向的架构方法，著重于重大中断后恢复服务与资讯。

DR 著重服务恢复，高可用性则著重服务持续性；两者互补，但在架构上彼此不同。

身分验证（Identity Authentication）

Cyberhood 平台在考虑允许存取适用的平台资源或服务之前，用以验证参与使用者或应用身分的程序。

授权（Authorization）

平台用以判断已验证身分是否被允许存取应用、服务、资讯资源或其他受保护资源，或对其执行适用动作的程序。

Independent Firewall

Cyberhood 安全架构中的主机保护能力，作为更广泛分层安全模型的一部分，用以保护参与的分散式主机。

企业协作（Enterprise Collaboration）

原生平台能力，连结人员、身分、通讯、企业资讯、分享、搜寻、版本管理、工作空间、应用与组织流程。

在 Cyberhood 架构中，协作连结人员、资讯与工作，而非仅作为孤立的通讯功能。

我的空间（My Space）

Cyberhood 中代表使用者个人资讯环境的逻辑工作空间。

公共空间（Public Space）

Cyberhood 中供较广泛且经授权之组织成员使用资讯的逻辑工作空间。

我分享的空间（Sharing With Space）

Cyberhood 的逻辑工作空间关系，代表我分享给其他人的资讯。

分享给我的空间（Shared From Space）

Cyberhood 的逻辑工作空间关系，代表其他人分享给我的资讯。

企业应用生态系统与整合

与 Cyberhood 平台共同运作的专业化企业应用集合，包括 Workflow、Project Management、CRM、ERP 及相关组织能力。

应用在参与共同平台架构的同时，仍保有各自专业化的业务责任。

企业应用整合（Enterprise Application Integration）

Cyberhood 已实作的平台能力，透过共享企业流程与整合机制连接多个专业化企业应用，同时保留各应用的专业化业务责任。

企业整合服务（Enterprise Integration Services）

Cyberhood 用以连接参与企业应用与服务的已实作整合能力，包括 API Integration、Transaction Orchestration、Enterprise Service Bus（ESB）、Message Bus 与 Automatic Cross-Application Synchronization。

API Integration

透过已定义的应用介面，使参与应用与服务交换功能能力与资讯的整合能力。

交易编排（Transaction Orchestration）

协调跨越应用边界之业务活动与交易关系的整合能力。

Enterprise Service Bus（ESB）

使参与服务与应用在 Cyberhood 企业应用环境中进行协调式互动的共享企业整合能力。

Message Bus

支援参与应用与平台元件之间讯息通讯与事件交换的讯息型整合能力。

Automatic Cross-Application Synchronization

依整合式企业流程需求，维持参与应用之间相关资讯与流程状态关系的已实作能力。

跨应用流程协调（Cross-Application Process Orchestration）

协调跨越多个专业化应用的企业流程。在 Cyberhood 中，工作流程／电子签核可作为跨应用流程协调能力，连接业务活动、电子签核、组织授权、电子文件、内部稽核、内部控制与后续应用处理。

Cyberhood SDK

Cyberhood 提供的共同软体开发基础，使额外应用可与 Cyberhood 分散式平台服务及参与的平台资源建立关系。

Distributed Application Framework

一套架构框架，使 Cyberhood 应用可依应用设计，与身分验证、Distributed Service Selection、应用处理、平台资源及分散式基础架构建立关系并运作。

Distributed Service Selection（分散式服务选择）

Cyberhood 平台机制，使应用可依平台模型辨识适当的参与服务主机，并在适用时考量距离或效能。

Distributed Service Selection 不应被解读为通用的自动应用容错移转。

私有企业部署（Private Enterprise Deployment）

Cyberhood 主要运作于组织所控制基础架构上的部署模式。参与的基础架构可位于一个或多个组织地点。

私有部署不等于单一站点部署。

私有云部署（Private Cloud Deployment）

Cyberhood 运作于由组织控制或专用的云端导向基础架构上，同时维持整体 Cyberhood 平台架构的部署模式。

混合云部署（Hybrid Cloud Deployment）

依企业需求，使私有基础架构与外部或云端导向基础架构共同参与整体 Cyberhood 平台架构的部署模式。

多站点企业部署（Multi-Site Enterprise Deployment）

总部、分公司、区域设施或其他组织站点共同参与 Cyberhood 平台架构的部署方式。

参与站点不一定需要相同的实体基础架构或相同的服务配置。

复原导向部署（Recovery-Oriented Deployment）

一种部署架构，用以提供重大中断后恢复适用服务与资讯所需的资源及架构关系。

复原导向部署与高可用性架构互补，但其本身并不定义通用的复原目标、RPO、RTO 或自动地理容错移转。

Protected Information Layer（受保护资讯层）

Cyberhood SPAN 对适用企业资讯提供受保护分段、加密、分散式配置、门槛式重建、装置层级容错与保护状态复原的架构层。

Protected Information Layer 与实体储存基础架构相关，但在架构上彼此不同。

受保护资讯（Protected Information）

透过适用的 Cyberhood 授权、安全与资讯保护关系处理的企业资讯。当 SPAN 保护适用时，受保护资讯可参与分段、加密、分散式配置、门槛式重建、已设定容错及保护状态复原。

并非每一个应用或每一类资讯都会自动受到 SPAN 保护。

模组化扩充（Modular Expansion）

随需求演进，透过增加运算资源、储存资源、分散式节点、组织站点或平台容量来扩充 Cyberhood 的架构能力。

模组化扩充在允许实体资源与部署拓朴演进的同时，维持整体架构模型。增加储存资源会创造更多架构选项，但不会自动提高 SPAN 的容错能力。

业务服务（Business Services）

由企业应用与底层 Cyberhood 平台架构所支援的组织活动、营运能力与业务责任。

Cyberhood 架构框架（Cyberhood Architecture Framework, CAF）

描述分散式基础架构、分散式平台服务、协作与资讯服务、企业应用及业务服务如何在 Cyberhood 分散式企业平台中相互关联的逻辑架构参考框架。

CAF 亦描述涉及身分、安全、受保护资讯、分散式应用架构与部署架构的跨层关系。CAF 是逻辑架构框架，而非强制性的实体部署拓朴。

附录 B

参考架构

本附录提供概念性参考架构，汇整本白皮书所定义的主要架构关系。这些模型说明 Cyberhood 基础架构、平台服务、资讯、安全、应用与组织环境之间的逻辑关系。它们是参考模型，而非强制性的实体拓朴；实际实作可依企业需求、参与资源、服务配置、资讯配置与部署设计而异。

B.1 Cyberhood 企业平台参考架构

目的 — 说明组织使用者与业务服务如何透过专业化企业应用、协作与资讯服务、共用平台服务及分散式基础架构运作。

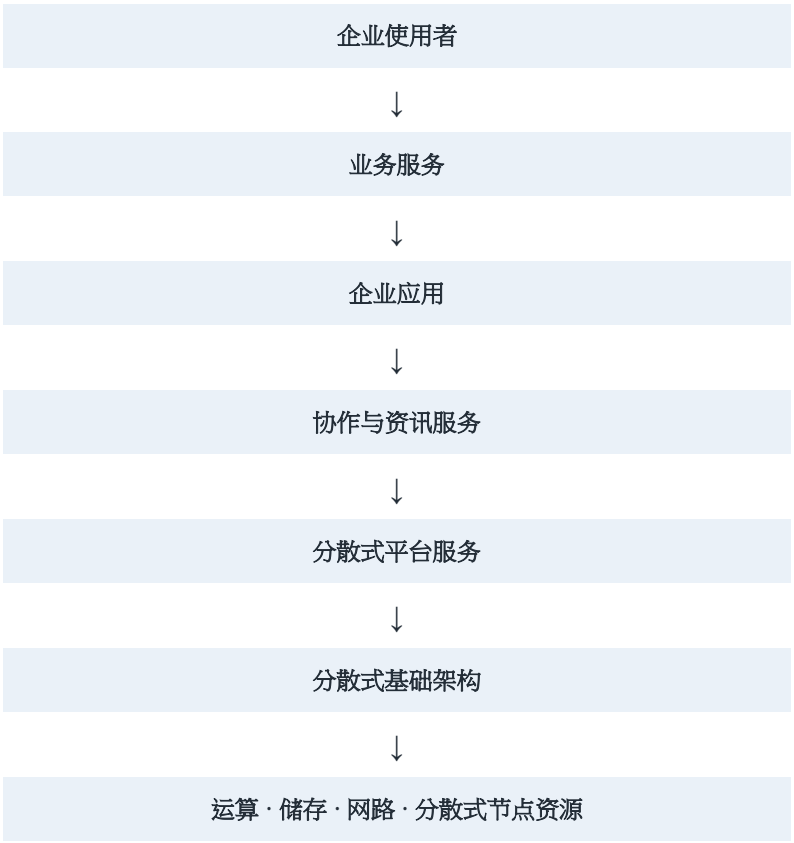


图 B-1 — Cyberhood 企业平台参考架构

安全、身分与授权，以及受保护资讯，作为彼此相关的跨层责任运作。

关键关系 — 业务服务代表平台所支援的组织能力。企业应用保有专业化的业务责任，同时与共用平台能力建立关系。分散式平台服务与分散式基础架构则为更高层级的企业能力提供共享架构基础。

业务责任各自专业化；平台服务共享。

架构考量 — 此模型分离架构责任，但不隔离架构参与。安全跨越各层运作，而非独立的应用层。适用时，受保护资讯可透过 Cyberhood SPAN Protected Information Layer 参与协作与应用。

责任分离不代表架构必须分离。

B.2 企业应用整合参考架构

目的 — 说明专业化企业应用如何透过已实作的企业整合服务参与共享企业流程，同时保留其专业化业务责任。

专业化企业应用 ↔ 共享企业流程与工作流程整合 ↔ 企业整合服务 ↔ Cyberhood 平台核心服务 ↔ Cyberhood SPAN ↔ 分散式基础架构

企业整合服务包括 API Integration、Transaction Orchestration、Enterprise Service Bus（ESB）、Message Bus 通讯与 Automatic Cross-Application Synchronization。工作流程／电子签核为电子签核、电子文件、组织授权、内部稽核、内部控制与后续业务处理提供跨应用流程协调关系。

关键关系 — 应用维持专业化；企业流程可跨越应用边界；整合服务连接 API、交易、讯息、资讯流与流程状态；共同平台服务由参与应用共享。应用整合不要求功能趋同。

B.3 分散式基础架构参考架构

目的 — 说明 Cyberhood 节点角色与基础架构资源如何参与更广泛的平台环境。

参与节点角色	分散式资源
Master Nodes Slave Nodes 分散式本地节点（DLN）	运算 储存 网路

图 B-2 — 分散式基础架构参考架构

Cyberhood 平台 ↔ 参与节点与资源 ↔ 组织站点／部署环境

关键关系 — 节点角色代表架构参与，而非通用硬体配置。分散式本地节点依被指派的服务与部署需求，将 Cyberhood 平台延伸至组织地点。各站点参与的运算、储存与网路资源可有所不同。

架构考量 — 共同平台架构不要求各站点采用相同架构。多个参与资源可提供韧性的架构基础，但实际服务持续性取决于服务设定与部署设计。分散式本地节点是整体平台架构的一部分，而非独立平台。

分散式架构 ≠ 自动高可用性。

B.4 受保护资讯参考架构

目的 — 说明以身分为基础的存取控制、企业资讯使用与 Cyberhood SPAN Protected Information Layer 之间的关系。

存取控制关系	受保护资讯关系
身分 验证 授权 应用与协作 企业资讯	企业资讯 Cyberhood SPAN 分段与加密 分散式配置 门槛式重建 保护状态复原

图 B-3 — 受保护资讯参考架构

存取控制与受保护资讯架构彼此相关，但在架构上不同。

关键关系 — 身分、验证与授权治理谁可以存取企业资讯。应用与协作服务决定经授权资讯如何参与组织工作。Cyberhood SPAN 则治理适用的受保护资讯如何被分段、加密、分散、重建与复原。

架构考量 — SPAN 不会自动保护每个应用或资讯类别。地理分散的受保护资讯配置不会自动建立地理服务容错移转。增加储存资源也不会自动提高已设定的容错能力。

资讯是逻辑企业资源；储存是基础架构资源。

B.5 多站点企业参考架构

目的 — 说明地理或组织上分散的地点如何参与共同的 Cyberhood 平台架构。

企业地点	平台参与
总部	分散式本地节点
分公司	参与平台节点
区域设施	Cyberhood 平台服务
分散式站点	分散式基础架构资源

图 B-4 — 多站点企业参考架构

共同企业架构不要求各站点具有相同的基础架构。

关键关系 — 组织站点可参与共同平台，而不要求每个地点具备相同基础架构。服务配置、应用配置与受保护资讯配置可因站点而异。使用者可依身分与授权关系，跨地点参与协作与企业资讯服务。

架构考量 — 多站点架构不会自动代表 Active-Active 区域服务、通用应用复写或自动地理容错移转。地理基础架构分布、地理服务分布与地理受保护资讯分布彼此相关，但在架构上不同。

使用者位置 ≠ 资讯位置 · 应用位置 ≠ 完整资讯位置

参考架构原则

逻辑架构与实体拓朴彼此相关，但在架构上不同。

安全跨越整体架构运作，而非独立的一层。

服务配置与受保护资讯配置彼此相关，但不同。

分散式架构提供基础；部署设计决定营运行为。

一个平台架构 — 多种部署模式。

附录 C

技术重点

本附录提供本白皮书主要 Cyberhood 架构能力的技术摘要，作为技术评估的精简参考；内容汇整架构特性与关系，而非取代正文中的详细说明与实作考量。

C.1 分散式架构

- 分散式基础架构依部署需求纳入 Master Nodes、Slave Nodes、分散式本地节点、运算资源、储存资源、网路资源及参与的组织地点。
- 原生分散式设计 — 分散式资源是平台基础的一部分，而非中央集中式架构的选配延伸。
- 共同平台架构的设计，使企业服务降低对单一伺服器、储存装置或组织地点的依赖。
- 可透过增加节点、储存资源、参与站点与平台容量进行模组化扩充。
- 分散式架构为韧性与多站点营运提供基础，但其本身不保证高可用性或自动地理容错移转。

C.2 高可用性与韧性

- 高可用性架构透过参与的分散式资源、故障侦测、隔离、重新分配、复原与容量恢复，支援服务持续性。
- 分散式架构中的连线、资料与运算负载平衡概念。
- 高可用性著重服务持续性；复原导向架构著重服务恢复。
- 在适当的服务与资源被设定参与时，分散式部署可降低对个别基础架构元件的依赖。
- 仅有多个资源并不构成高可用性。实际持续性取决于部署设计、参与服务、资源设定与适用的故障条件。

C.3 安全与资讯保护

- 身分验证与授权作为基础存取控制关系：身分 → 验证 → 授权 → 受保护资源。
- 参与分散式主机的安全通讯机制与 Independent Firewall 保护。
- 在受保护加密储存之前进行恶意程式扫描。
- Cyberhood SPAN 作为 Protected Information Layer，对适用企业资讯支援受保护分段、加密、分散式配置、门槛式重建、已设定容错及保护状态复原。
- 安全跨越架构各层运作，而非独立的应用层。
- 受保护资讯架构无法消除所有安全风险，且 SPAN 不会自动套用至每个应用或资讯类别。

C.4 协作与资讯服务

- Enterprise Mail 与 Enterprise Messenger 提供组织通讯。
- 档案管理、版本控制、全文搜寻、分享与跨平台资讯存取。
- 逻辑工作空间模型：我的空间（My Space）· 公共空间（Public Space）· 我分享的空间（Sharing With Space）· 分享给我的空间（Shared From Space）。
- 企业资讯生命周期：建立 → 储存 → 分享 → 协作 → 版本管理 → 搜寻 → 保护。
- 协作服务在整体平台架构中连结人员、通讯、企业资讯与组织工作。
- 工作空间是逻辑资讯环境，而非实体站点边界。

C.5 企业应用与整合

企业应用生态系统与整合包括 EIP、工作流程／电子签核、ERP、CRM、专案管理、通讯与协作，以及其他整合式企业应用。

企业应用整合是已实作的平台能力，连接应用 API、交易、讯息、资讯流与企业流程。

企业整合服务包括 API Integration、Transaction Orchestration、Enterprise Service Bus（ESB）、Message Bus 通讯与 Automatic Cross-Application Synchronization。

工作流程／电子签核既是专业化应用能力，也是跨应用流程协调机制，连接电子签核、电子文件、组织授权、内部稽核、内部控制与后续业务处理。

Cyberhood SDK 与分散式应用框架提供开发基础，使额外应用可依应用设计与平台及整合能力建立关系并运作。

业务责任各自专业化；平台服务共享。应用整合不要求功能趋同。

C.6 部署与扩充

- 架构部署模式包括私有企业、私有云、混合云、多站点企业、分散式本地节点与复原导向部署。
- 不依赖特定供应商的概念性混合架构，不受特定公有云供应商绑定。
- 逻辑平台架构与实体部署拓朴分离。
- 一个平台架构 — 多种部署模式。
- 模组化架构可随运算容量、储存资源、分散式节点、组织站点、应用与企业需求持续演进。
- 私有部署 ≠ 单一站点部署。逻辑一致性不要求实体一致。
- 地理基础架构分布、地理服务分布与地理受保护资讯分布彼此相关，但在架构上不同。

C.7 架构摘要

Cyberhood 技术能力被设计为协调一致的分散式企业架构之一部分，而非彼此孤立的技术领域。

分散式基础架构 → 共用平台服务 → 安全与受保护资讯 → Enterprise Integration Services → 协作与企业资讯 → 整合式企业应用 → 协调式企业流程 → 业务营运

Cyberhood 的架构价值不仅来自个别能力，更来自连结这些能力的关系。

附录 D

Cyberhood 架构框架（Cyberhood Architecture Framework, CAF）

D.1 Cyberhood 架构框架的目的

Cyberhood 架构框架（CAF）提供统一的逻辑参考模型，用以理解分散式基础架构、共用平台服务、企业整合服务、协作、企业资讯、专业化应用、安全与部署架构，如何共同参与协调一致的企业平台。CAF 描述架构责任与关系，而非规定单一强制实作拓朴，因此可应用于不同的组织环境、基础架构设定、部署模式及企业演进阶段。

CAF 定义架构关系 — 而非强制性的实体配置。

此框架描述有哪些责任以及彼此如何关联；部署设计则决定它们在何处运作。

D.2 CAF 分层架构

CAF 将 Cyberhood 架构组织为逻辑责任层与跨层关系。企业整合服务连接专业化应用、共享企业流程与共同平台能力，同时保留业务责任的区分。

第 5 层 — 业务服务

↓

第 4 层 — 企业应用

↓

第 3 层 — 协作与资讯服务

↓

第 2 层 — 分散式平台服务

↓

第 1 层 — 分散式基础架构

图 D-1 — Cyberhood 架构框架概观

跨层责任：身分与授权 · 安全架构 · 受保护资讯（Cyberhood SPAN）。部署模式决定参与的实体拓朴。

CAF 各层代表逻辑责任，不一定对应专用的实体系统。

D.3 第 1 层 — 分散式基础架构

第 1 层提供 CAF 的实体与分散式基础架构基础。依部署需求，它包括参与的运算、储存、网路资源、Master Nodes、Slave Nodes、分散式本地节点及其他基础架构资源。本层为分散式资源参与、模组化扩充、多站点营运，以及在适当设定下的高可用性设计提供架构基础。

分散式基础架构提供韧性的基础；其本身并不自动构成高可用性。

D.4 第 2 层 — 分散式平台服务

第 2 层提供运作于分散式基础架构之上的共用平台能力，以支援更高层级的协作、资讯、应用与业务责任。这些能力包括身分验证、授权、索引、分散式储存服务、工作流程、讯息传递、SDK 服务、管理及本白皮书所述其他共用平台服务。本层的架构目的，是提供不需要由每个业务应用各自重新建立的共享能力。

平台服务是共享的架构能力，而非特定业务责任。

D.5 第 3 层 — 协作与资讯服务

第 3 层将组织使用者与通讯、协作、企业资讯、分享、搜寻、版本管理及逻辑工作空间服务连结。它包括 Enterprise Mail、Enterprise Messenger、档案管理、我的空间（My Space）、公共空间（Public Space）、我分享的空间（Sharing With Space）、分享给我的空间（Shared From Space）、版本控制、全文搜寻及相关协作能力。本层代表人员、通讯、企业资讯与组织工作之间的架构关系。

通讯连结人员；协作连结人员、资讯与工作。

工作空间是逻辑资讯环境，而非实体站点边界。

D.6 第 4 层 — 企业应用

第 4 层包含将平台能力转化为组织流程与业务功能的专业化企业应用，包括 EIP、工作流程／电子签核、ERP、CRM、专案管理、通讯与协作及相关企业应用能力。应用保有专业化业务责任，同时参与共享的工作流程、整合、资讯与平台关系。

业务责任各自专业化；平台服务共享。

应用参与平台，但不定义平台。

D.7 企业应用整合架构

企业应用整合是平台层级的架构关系，透过共享企业流程与已实作的企业整合服务连接专业化应用。

专业化应用 <-> 共享企业流程与工作流程整合 <-> API Integration / Transaction Orchestration / ESB / Message Bus / Automatic Cross-Application Synchronization <-> Platform Core Services

工作流程／电子签核提供跨应用流程协调，涵盖电子签核、电子文件、组织授权、内部稽核、内部控制与后续业务处理。

平台连接专业化应用，而不消除其专业化责任。

D.8 第 5 层 — 业务服务

第 5 层代表 Cyberhood 架构最终支援的组织活动、营运能力与业务责任。在此层，企业应用、协作、资讯与平台能力共同支援组织流程与业务营运。因此，CAF 将科技架构与企业活动连结，而不把业务责任视为实作意义上的科技层。

D.9 跨层安全架构

在 CAF 中，安全是跨层架构责任，而非独立的应用层。

身分 → 验证 → 授权 → 受保护资源

安全机制跨越不同架构责任参与，包括安全通讯、Independent Firewall 主机保护、恶意程式防护、活动纪录与受保护资讯。不同控制措施依参与的平台服务、应用、资讯资源、基础架构资源与部署设计而适用。

安全不是单一边界，而是跨架构层的关系。

安全控制保护元件；安全架构保护关系。

D.10 受保护资讯架构

CAF 将企业资讯视为逻辑企业资产，并使其参与协作、应用、安全与组织流程。

建立 → 储存 → 分享 → 协作 → 版本管理 → 搜寻 → 保护

Cyberhood SPAN 为适用的企业资讯提供受保护资讯层（Protected Information Layer）。

企业资讯 → Cyberhood SPAN → 分段 → 加密 → 分散式配置 → 门槛式重建 → 保护状态复原

参与的储存资源在此逻辑受保护资讯架构之下提供基础容量。SPAN 不会自动套用至每个应用或资讯类别，且地理分散的受保护资讯配置不会自动建立地理服务容错移转。

资讯是逻辑企业资源；储存是基础架构资源。

受保护资讯配置与服务配置彼此相关，但在架构上不同。

D.11 分散式应用架构

CAF 定义一种分散式应用关系，使应用可透过 Cyberhood SDK 与 Distributed Application Framework，与共用平台服务及分散式基础架构建立关系并运作。

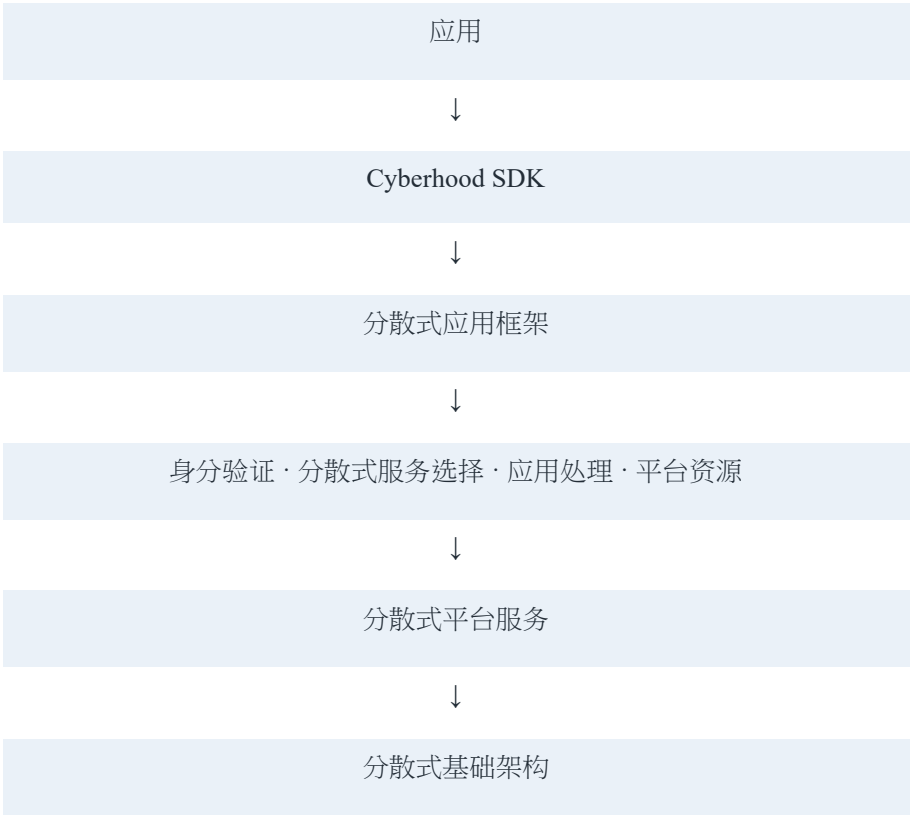


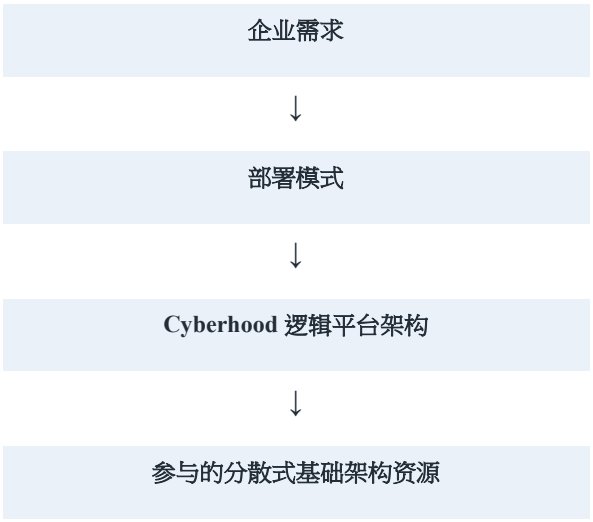
图 D-2 — 分散式应用架构

应用实际使用哪些平台能力，取决于其设计与需求。

分散式服务选择（Distributed Service Selection）不代表通用的自动应用容错移转。扩充性是平台能力，但不保证每一项未来应用需求都会自动获得满足。

D.12 部署架构

CAF 将逻辑平台架构与实体部署拓朴分离。



CAF 部署关系

本白皮书所述的支援架构模式包括私有企业、私有云、混合云、多站点企业、分散式本地节点与复原导向部署。地理基础架构分布、服务分布与受保护资讯分布彼此相关，但在架构上不同。

一个平台架构 — 多种部署模式。

逻辑一致性不要求实体一致。

部署改变架构运作的位置 — 而不是架构本质。

D.13 CAF 架构原则

- 原生分散式设计 — 分散式基础架构是平台基础的一部分，而非选配延伸。
- 平台优先于产品 — 个别功能与应用参与更广泛的企业平台架构。
- 身分作为基础 — 身分连结使用者、组织角色、授权、应用、资讯与企业资源。
- 资讯作为企业资产 — 企业资讯参与储存、协作、搜寻、应用、安全与组织流程。
- 安全即架构 — 安全跨越架构各层运作，而非单一边界或独立层。
- 协作作为原生能力 — 通讯、资讯、分享、工作空间与组织互动共同参与企业平台。
- 业务责任各自专业化；平台服务共享 — 应用保有专业化业务责任，同时参与共用平台能力。
- 一个平台架构 — 多种部署模式 — 不同实体部署环境可套用同一套更广泛的逻辑平台架构。
- 模组化演进 — 运算、储存、分散式节点、组织地点与平台容量可随需求变化而演进。
- 为未来开发提供扩充性 — Cyberhood SDK 与 Distributed Application Framework 为额外应用能力提供架构基础。

这些原则共同将 CAF 定义为分散式企业运算的逻辑架构框架。CAF 提供共同模型，使基础架构、平台服务、企业资讯、安全、协作、应用、部署模式与业务责任，可在同一个协调式平台环境中被理解为彼此相关的架构领域。

CAF 定义使专业化企业能力得以在同一套分散式企业架构中运作的关系。

D.14 CAF 架构关系摘要

Cyberhood 架构框架可透过七项主要关系加以概括：

平台关系

分散式基础架构 → 分散式平台服务 → 协作与资讯服务 → 企业应用 → 业务服务

安全关系

身分 → 验证 → 授权 → 受保护资源

资讯关系

建立 → 储存 → 分享 → 协作 → 版本管理 → 搜寻 → 保护

受保护资讯关系

企业资讯 → SPAN → 分段 → 加密 → 分散式配置 → 重建 → 复原

应用关系

应用 → Cyberhood SDK → 分散式应用框架 → 平台服务 → 分散式基础架构

企业整合关系

专业化应用 ↔ 共享企业流程与工作流程整合 ↔ API Integration / Transaction Orchestration / ESB / Message Bus / Automatic Cross-Application Synchronization ↔ Platform Core Services

部署关系

企业需求 → 部署模式 → 逻辑平台架构 → 分散式基础架构资源

这些关系构成 CAF 的架构核心。

Cyberhood 架构框架 — 分散式企业营运的一套逻辑架构。

CAF 定义分散式基础架构、平台服务、企业资讯、安全、协作、应用与部署模式如何在同一套协调式企业架构中参与的架构关系。

Cyberhood 分散式企业平台

架构原则 · 企业价值 · Kinghood Technology

Cyberhood 架构原则

- 原生分散式设计
- 平台优先于产品
- 身分作为基础
- 资讯作为企业资产
- 安全即架构
- 协作作为原生能力
- 业务责任各自专业化；平台服务共享
- 一个平台架构 — 多种部署模式
- 模组化演进
- 为未来开发提供扩充性

Cyberhood 的企业价值

- 统一架构 — 降低碎片化、复杂度与整合负担。
- 营运持续性 — 支援服务持续与复原导向营运。
- 资讯保护 — 透过分层安全与 Cyberhood SPAN 保护适用的企业资讯。
- 业务敏捷性 — 随需求演进调整应用、服务与部署架构。
- 可扩充成长 — 在共同平台架构中扩充使用者、资讯、资源与据点。

Cyberhood

Cyberhood 是一套分散式企业平台架构，连结基础架构、平台服务、企业资讯、安全、协作、应用与业务营运。

其设计旨在支援目前的企业需求，同时提供可随未来组织与科技需求持续演进的架构基础。

Kinghood Technology

网站：www.kinghood.com
电子邮件：sales@kinghood.com

Copyright © 2026 Kinghood Technology. All rights reserved.

一个分散式平台。一套企业架构。为持续演进而打造。