# Hybrid Cloud

**MỤC LỤC**  
1. Mở đầu  
2. Cơ sở lý thuyết  
  2.1. Khái niệm và đặc điểm của Hybrid Cloud  
  2.2. So sánh Hybrid Cloud với Public Cloud và Private Cloud  
3. Kiến trúc kỹ thuật  
  3.1. Các thành phần chính trong kiến trúc Hybrid Cloud  
  3.2. Mô hình triển khai Hybrid Cloud  
  3.3. Các công nghệ hỗ trợ trong Hybrid Cloud  
4. Ứng dụng thực tế trong doanh nghiệp  
  4.1. Các kịch bản sử dụng Hybrid Cloud  
  4.2. Case study từ các doanh nghiệp lớn  
5. Bảo mật và tuân thủ  
  5.1. Rủi ro bảo mật trong mô hình Hybrid Cloud  
  5.2. Giải pháp đảm bảo an ninh và quản lý dữ liệu  
  5.3. Tuân thủ các tiêu chuẩn và quy định  
6. Kết luận và hướng phát triển

## 1. Mở đầu

Điện toán đám mây (cloud computing) đã trở thành một xu hướng công nghệ chủ đạo trong hơn một thập kỷ qua, cung cấp mô hình truy cập qua mạng tới các tài nguyên tính toán dùng chung một cách thuận tiện, linh hoạt theo yêu cầu[[1]](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf#:~:text=Cloud%20computing%20is%20a%20model,models%2C%20and%20four%20deployment%20models). Với sự phát triển nhanh chóng của hạ tầng và dịch vụ đám mây công cộng, nhiều doanh nghiệp đã chuyển đổi một phần hoặc toàn bộ hệ thống của mình lên đám mây nhằm tận dụng khả năng mở rộng linh hoạt và mô hình chi phí theo nhu cầu. Tuy nhiên, không phải mọi ứng dụng hay dữ liệu đều có thể đặt hoàn toàn trên đám mây công cộng do các yêu cầu về bảo mật, độ trễ hoặc tuân thủ quy định. Trong bối cảnh đó, mô hình **đám mây lai (hybrid cloud)** đã ra đời, kết hợp ưu điểm của cả đám mây riêng và đám mây công cộng để đáp ứng tốt hơn nhu cầu doanh nghiệp[[2]](https://developers.redhat.com/topics/hybrid-cloud-architecture#:~:text=Hybrid%20cloud%20setups%20have%20become,sensitivity%20and%20high%20volume%20requirements).

Sự xuất hiện của hybrid cloud xuất phát từ thực tế rằng doanh nghiệp cần một giải pháp cân bằng: vừa khai thác được tài nguyên gần như vô hạn của đám mây công cộng, vừa duy trì được mức độ kiểm soát, bảo mật đối với hạ tầng nội bộ. Ban đầu, khái niệm hybrid cloud gắn liền với ý tưởng *cloud bursting* – doanh nghiệp vận hành ứng dụng trên hạ tầng tại chỗ và "bùng nổ" sang đám mây công cộng khi nhu cầu tài nguyên tăng đột biến[[3]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=NIST%27s%20original%20hybrid%20cloud%20definition,capacity%20wherever%20it%20was%20cheapest). Ví dụ, một trung tâm dữ liệu nội bộ có thể xử lý tải cơ bản, nhưng khi lượng người dùng tăng vọt, hệ thống có thể tự động mở rộng lên đám mây công cộng để đáp ứng mà không cần đầu tư thêm máy chủ cục bộ. Ý tưởng này cho thấy tính linh hoạt của hybrid cloud trong việc xử lý tải đỉnh. Bên cạnh đó, hybrid cloud còn giúp doanh nghiệp tránh phụ thuộc hoàn toàn vào một nhà cung cấp, tăng khả năng dự phòng và đáp ứng các yêu cầu về vị trí lưu trữ dữ liệu.

Thực tế cho thấy hybrid cloud ngày càng được áp dụng rộng rãi. Các khảo sát gần đây cho thấy phần lớn các tổ chức lớn đã và đang triển khai mô hình đám mây lai. Chẳng hạn, một khảo sát năm 2020 cho thấy có đến 63% lãnh đạo CNTT đã triển khai hybrid cloud, và 54% trong số còn lại cũng có kế hoạch áp dụng[[2]](https://developers.redhat.com/topics/hybrid-cloud-architecture#:~:text=Hybrid%20cloud%20setups%20have%20become,sensitivity%20and%20high%20volume%20requirements). Điều này phản ánh niềm tin rằng hybrid cloud mang lại sự linh hoạt vượt trội, kết hợp tốc độ mở rộng của đám mây công cộng với tính bảo mật, tuân thủ của đám mây riêng. Hybrid cloud không chỉ là giải pháp tình thế, mà đang trở thành chiến lược dài hạn giúp doanh nghiệp chuyển đổi số một cách an toàn và hiệu quả. Phần tiếp theo của luận văn sẽ trình bày cơ sở lý thuyết về mô hình này, so sánh với các mô hình đám mây khác, kiến trúc kỹ thuật, ứng dụng thực tiễn, cũng như các vấn đề về bảo mật và tuân thủ trong hybrid cloud.

## 2. Cơ sở lý thuyết

### 2.1. Khái niệm và đặc điểm của Hybrid Cloud

**Hybrid Cloud** (đám mây lai) là một trong bốn mô hình triển khai điện toán đám mây được định nghĩa bởi NIST (Viện Tiêu chuẩn và Công nghệ Hoa Kỳ). Theo đặc tả NIST SP 800-145, *“hạ tầng cloud lai là sự kết hợp của hai hoặc nhiều hạ tầng đám mây riêng biệt (riêng, cộng đồng hoặc công cộng), tồn tại như những thực thể riêng nhưng được liên kết với nhau bởi công nghệ chuẩn hoặc công nghệ độc quyền cho phép dữ liệu và ứng dụng có thể di chuyển qua lại”*[[4]](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf#:~:text=Hybrid%20cloud,for%20load%20balancing%20between%20clouds). Nói cách khác, hybrid cloud tích hợp cả **đám mây riêng** (private cloud) và **đám mây công cộng** (public cloud) trong một kiến trúc thống nhất, cho phép chia sẻ tải công việc (workload), dữ liệu giữa hai môi trường này một cách linh hoạt. Các thành phần trong mô hình hybrid có thể bao gồm hạ tầng tại chỗ (on-premises), đám mây riêng của doanh nghiệp, và dịch vụ từ một hoặc nhiều nhà cung cấp đám mây công cộng, được kết nối với nhau qua mạng và các công cụ tích hợp.

Đặc điểm nổi bật của hybrid cloud nằm ở khả năng **di động và linh hoạt** của ứng dụng và dữ liệu giữa các môi trường. Nhờ được liên kết bằng các công nghệ tiêu chuẩn (ví dụ: giao diện API thống nhất, định dạng đóng gói ứng dụng như container), ứng dụng có thể triển khai ở cả hai môi trường và di chuyển khi cần thiết (như trong kịch bản cloud bursting)[[5]](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf#:~:text=Hybrid%20cloud,libraries%2C%20services%2C%20and%20tools%20from)[[3]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=NIST%27s%20original%20hybrid%20cloud%20definition,capacity%20wherever%20it%20was%20cheapest). Hybrid cloud cho phép doanh nghiệp tận dụng **độ mở rộng (scalability)** và **tính sẵn có (availability)** gần như không giới hạn của đám mây công cộng, đồng thời vẫn duy trì **mức độ kiểm soát, bảo mật cao** đối với những hệ thống hoặc dữ liệu nhạy cảm bằng cách giữ chúng trên đám mây riêng hoặc tại chỗ[[2]](https://developers.redhat.com/topics/hybrid-cloud-architecture#:~:text=Hybrid%20cloud%20setups%20have%20become,sensitivity%20and%20high%20volume%20requirements). Chính sự kết hợp này mang lại **tính linh hoạt (flexibility)** vượt trội – doanh nghiệp có thể lựa chọn môi trường tối ưu cho từng loại workload: phần ít nhạy cảm hoặc đòi hỏi tài nguyên lớn có thể đưa lên public cloud để tiết kiệm chi phí, trong khi phần cần bảo mật cao hoặc tuân thủ nghiêm ngặt thì giữ ở private cloud[[6]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=A%20hybrid%20cloud%20model%20allows,as%20PaaS%20and%20IaaS%20services).

Bên cạnh đó, hybrid cloud còn có đặc điểm là **tính phức tạp trong quản lý** cao hơn so với mô hình thuần nhất. Do bao gồm nhiều môi trường khác biệt, việc quản lý một hệ thống hybrid đòi hỏi các giải pháp quản lý và giám sát hợp nhất, đảm bảo ứng dụng hoạt động thông suốt qua các hạ tầng. Công nghệ ảo hóa và container hóa ngày càng đóng vai trò quan trọng trong hybrid cloud, giúp đóng gói ứng dụng cùng môi trường chạy của nó để có thể triển khai nhất quán trên nhiều nền tảng. Ví dụ, sự phổ biến của Docker container và Kubernetes đã nâng cao khả năng **portability** (di động) của ứng dụng giữa on-premises và các đám mây khác nhau[[7]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=The%20widespread%20adoption%20of%20containers,testing%2C%20and%20finally%20to%20production). Nhờ container, các ứng dụng cùng toàn bộ phụ thuộc có thể được chuyển từ môi trường phát triển sang thử nghiệm rồi sản xuất, bất kể chạy trên máy vật lý, private cloud hay public cloud, mà vẫn đảm bảo tính nhất quán về cấu hình và hiệu năng[[7]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=The%20widespread%20adoption%20of%20containers,testing%2C%20and%20finally%20to%20production). Những nỗ lực tiêu chuẩn hóa như Open Container Initiative (OCI) đã góp phần tạo ra định dạng container và môi trường chạy thống nhất, mở đường cho hệ sinh thái công cụ đa dạng hỗ trợ triển khai đa đám mây[[8]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=Specifications%20developed%20under%20the%20auspices,stable%20runtime%20and%20image%20specs).

Tóm lại, hybrid cloud là mô hình đám mây kết hợp, cho phép doanh nghiệp **“dùng đúng tài nguyên cho đúng việc”** – khai thác hạ tầng công cộng khi cần mở rộng nhanh và tiết kiệm chi phí, nhưng vẫn giữ được quyền kiểm soát trực tiếp với những tài sản số quan trọng. Mô hình này ngày càng phổ biến do phù hợp với lộ trình chuyển đổi số: nhiều tổ chức chọn hybrid cloud như bước đệm để từng bước đưa hệ thống lên mây một cách an toàn, thay vì chuyển đổi ồ ạt một lần[[9]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=defined%20by%20NIST.%20,allows%20users%20to%20migrate%20gradually)[[10]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=effective%20than%20private%20ones,allows%20users%20to%20migrate%20gradually).

### 2.2. So sánh Hybrid Cloud với Public Cloud và Private Cloud

Để hiểu rõ hơn vai trò của hybrid cloud, cần so sánh nó với hai mô hình triển khai truyền thống là public cloud (đám mây công cộng) và private cloud (đám mây riêng). Bảng dưới đây tóm tắt một số điểm khác biệt chính giữa ba mô hình này dựa trên các tiêu chí quan trọng:

*Bảng 1: So sánh đặc điểm giữa đám mây công cộng, đám mây riêng và đám mây lai (tổng hợp từ nguồn*[*[11]*](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Factors%3APublic%20Cloud%20Private%20Cloud%20Hybrid,portion%20shared%20with%20other%20clients)[*[12]*](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Setup%20Complexity%20Easy%20Complex%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies)*).*

| **Tiêu chí** | **Đám mây công cộng (Public Cloud)** | **Đám mây riêng (Private Cloud)** | **Đám mây lai (Hybrid Cloud)** |
| --- | --- | --- | --- |
| **Chủ sở hữu hạ tầng** | Nhà cung cấp dịch vụ cloud bên thứ ba[[11]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Factors%3APublic%20Cloud%20Private%20Cloud%20Hybrid,portion%20shared%20with%20other%20clients). Doanh nghiệp thuê tài nguyên dùng chung với khách hàng khác. | Doanh nghiệp (sở hữu hoặc thuê độc quyền một hạ tầng riêng)[[11]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Factors%3APublic%20Cloud%20Private%20Cloud%20Hybrid,portion%20shared%20with%20other%20clients). Chỉ phục vụ cho tổ chức duy nhất. | Kết hợp: một phần hạ tầng thuộc doanh nghiệp, một phần sử dụng của nhà cung cấp công cộng[[11]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Factors%3APublic%20Cloud%20Private%20Cloud%20Hybrid,portion%20shared%20with%20other%20clients). |
| **Quyền truy cập hạ tầng** | Không truy cập trực tiếp tầng vật lý; tài nguyên được cung cấp qua internet dưới dạng dịch vụ[[13]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Access%20Type%20No%20direct%20access,Complex%20Moderate%20Very%20complex%20Moderate). | Toàn quyền truy cập và kiểm soát hạ tầng (máy chủ, mạng) do thuộc sở hữu riêng[[13]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Access%20Type%20No%20direct%20access,Complex%20Moderate%20Very%20complex%20Moderate). | Truy cập một phần: doanh nghiệp kiểm soát phần private, còn phần public do nhà cung cấp quản lý[[13]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Access%20Type%20No%20direct%20access,Complex%20Moderate%20Very%20complex%20Moderate). |
| **Độ phức tạp triển khai** | Dễ dàng triển khai, thiết lập nhanh (nhà cung cấp lo phần hạ tầng)[[14]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=or%20organizations%20All%20companies%20or,to%20maintain%20Lower%20due%20to). | Phức tạp, tốn kém thời gian xây dựng và cấu hình hạ tầng riêng[[14]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=or%20organizations%20All%20companies%20or,to%20maintain%20Lower%20due%20to). | Trung bình: phải tích hợp hai môi trường, phức tạp hơn public nhưng đơn giản hơn xây toàn bộ private từ đầu[[14]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=or%20organizations%20All%20companies%20or,to%20maintain%20Lower%20due%20to). |
| **Bảo trì, vận hành** | Dễ dàng (nhà cung cấp chịu trách nhiệm bảo trì phần lớn)[[12]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Setup%20Complexity%20Easy%20Complex%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies). | Phức tạp (doanh nghiệp tự quản trị toàn bộ, từ phần cứng đến ứng dụng)[[12]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Setup%20Complexity%20Easy%20Complex%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies). | Trung bình: doanh nghiệp quản lý tích hợp, cần các công cụ giám sát cả hai môi trường[[12]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Setup%20Complexity%20Easy%20Complex%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies). |
| **Chi phí** | Hiệu quả cao, mô hình trả phí linh hoạt theo nhu cầu sử dụng (tiết kiệm nhờ kinh tế quy mô)[[12]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Setup%20Complexity%20Easy%20Complex%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies). | Chi phí cao, hiệu quả kinh tế thấp hơn do phải đầu tư hạ tầng riêng (phí cố định lớn)[[12]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Setup%20Complexity%20Easy%20Complex%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies). | Chi phí trung bình, kết hợp lợi ích của public cho phần không cần đầu tư và private cho phần quan trọng. Có thể tối ưu chi phí bằng cách chọn môi trường phù hợp cho từng workload[[12]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Setup%20Complexity%20Easy%20Complex%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies). |
| **Khả năng mở rộng** | Rất cao – tài nguyên gần như vô hạn từ nhà cung cấp, mở rộng linh hoạt theo nhu cầu[[15]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Cost%20Efficiency%20High%20Low%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies). | Hạn chế – chỉ mở rộng trong giới hạn hạ tầng sở hữu, nếu cần thêm phải mua sắm nâng cấp[[15]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Cost%20Efficiency%20High%20Low%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies). | Cao – phần công cộng có thể mở rộng linh hoạt, phần private vẫn có giới hạn nhưng tổng thể hệ thống có thể đáp ứng tốt nhu cầu tăng đột biến[[15]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Cost%20Efficiency%20High%20Low%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies). |
| **Độ tin cậy** | Phụ thuộc vào nhà cung cấp. Thông thường cao (hạ tầng lớn, dự phòng tốt) nhưng khách hàng ít kiểm soát trực tiếp. Khi sự cố xảy ra diện rộng có thể ảnh hưởng nhiều bên[[16]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Scalability%20High%20Low%20High%20Low,to%20maintain%20Lower%20due%20to)[[17]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Reliability%20Low%20High%20Moderate%20High,corporations%20%26%20multinational%20enterprises%20Companies). | Rất cao nếu được thiết kế tốt, doanh nghiệp toàn quyền kiểm soát các biện pháp dự phòng. Tuy nhiên chi phí để đạt độ tin cậy cao cũng lớn. | Trung bình – kết hợp dự phòng tại chỗ và trên cloud. Hệ thống phân tán giảm rủi ro điểm đơn lẻ, nhưng tích hợp phức tạp có thể phát sinh lỗi nếu không quản lý tốt. |
| **Bảo mật** | **Cao** ở mức hạ tầng (các nhà cung cấp lớn đầu tư mạnh vào bảo mật); tuy nhiên nếu xảy ra lỗ hổng hoặc tấn công, hậu quả có thể nghiêm trọng do dữ liệu nhiều khách hàng cùng nằm chung[[16]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Scalability%20High%20Low%20High%20Low,to%20maintain%20Lower%20due%20to). Doanh nghiệp phụ thuộc vào chính sách bảo mật của nhà cung cấp. | **Rất cao** – do môi trường dành riêng, doanh nghiệp tự thiết lập mọi chính sách bảo mật phù hợp nhu cầu. Ít nguy cơ từ bên ngoài, nhưng tốn kém nguồn lực duy trì mức bảo mật này[[16]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Scalability%20High%20Low%20High%20Low,to%20maintain%20Lower%20due%20to). | **Cao** – phần dữ liệu nhạy cảm được bảo vệ trong private cloud, phần công cộng được bảo mật bởi nhà cung cấp. Tổng thể nếu thiết kế tốt sẽ đáp ứng yêu cầu bảo mật và tuân thủ, nhưng phải chú ý bảo vệ kết nối giữa hai môi trường. |
| **Trường hợp phù hợp** | Hầu hết các công ty vừa và nhỏ, startup; các ứng dụng web, dịch vụ cần triển khai nhanh, linh hoạt. Phù hợp khi ưu tiên chi phí và mở rộng, không có yêu cầu đặc thù về dữ liệu[[18]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Public%20clouds%20are%20the%20best,be%20the%20way%20to%20go). | Các tổ chức lớn, doanh nghiệp tài chính, y tế... có dữ liệu nhạy cảm hoặc yêu cầu tùy biến cao, môi trường riêng biệt (do yêu cầu pháp lý hoặc hiệu năng đặc thù)[[18]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Public%20clouds%20are%20the%20best,be%20the%20way%20to%20go). | Doanh nghiệp cần đáp ứng đồng thời yêu cầu linh hoạt và bảo mật, chẳng hạn công ty có dữ liệu phải tuân thủ (tài chính, chính phủ) nhưng muốn tận dụng tài nguyên cloud; hoặc tổ chức đang trong giai đoạn chuyển đổi, muốn **di trú dần** một số ứng dụng lên cloud công cộng một cách an toàn[[19]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Best%20Fit%20Most%20companies%20Large,with%20very%20specific%20platform%20requirements)[[10]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=effective%20than%20private%20ones,allows%20users%20to%20migrate%20gradually). |

Nhìn chung, *đám mây công cộng* vượt trội về khả năng mở rộng và chi phí, phù hợp cho số đông ứng dụng không quá nhạy cảm về dữ liệu. *Đám mây riêng* đem lại quyền kiểm soát và bảo mật tối đa nhưng tốn kém và kém linh hoạt. *Đám mây lai* cố gắng kết hợp điểm mạnh của cả hai, cho phép vừa tiết kiệm chi phí vừa đảm bảo các yêu cầu đặc thù. Một phân tích chỉ ra rằng đối với đa số tổ chức, mô hình public hoặc hybrid (nghiêng về public) là lựa chọn kinh tế nhất, ngoại trừ các trường hợp đặc biệt đòi hỏi giải pháp riêng hoàn toàn[[9]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=defined%20by%20NIST.%20,allows%20users%20to%20migrate%20gradually). Tuy nhiên, hybrid cloud cũng đòi hỏi doanh nghiệp phải giải quyết các thách thức trong tích hợp và quản trị đa môi trường, điều sẽ được trình bày trong các phần sau.

## 3. Kiến trúc kỹ thuật

### 3.1. Các thành phần chính trong kiến trúc Hybrid Cloud

Kiến trúc kỹ thuật của một hệ thống hybrid cloud bao gồm nhiều thành phần trải rộng trên cả hạ tầng của doanh nghiệp và hạ tầng của nhà cung cấp dịch vụ đám mây. Về tổng thể, một hệ thống hybrid điển hình sẽ có các thành phần chính sau:

* **Hạ tầng tại chỗ (On-Premises Infrastructure)**: Bao gồm các máy chủ vật lý, máy ảo, thiết bị lưu trữ và mạng nằm trong trung tâm dữ liệu của doanh nghiệp hoặc đám mây riêng. Đây là nơi chạy các ứng dụng và lưu trữ dữ liệu nhạy cảm hoặc có yêu cầu đặc thù. Hạ tầng tại chỗ cung cấp mức độ kiểm soát và tùy biến cao, song chi phí đầu tư và duy trì cũng lớn. Doanh nghiệp có thể triển khai công nghệ ảo hóa (như VMware, KVM) hoặc nền tảng private cloud (như OpenStack) trên hạ tầng này để tối ưu tài nguyên và tạo môi trường tương thích với cloud[[20]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=On)[[21]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=However%2C%20on,premises%20infrastructure).
* **Đám mây công cộng (Public Cloud Services)**: Là hạ tầng và dịch vụ của một hoặc nhiều nhà cung cấp bên ngoài (AWS, Microsoft Azure, Google Cloud, v.v.). Các dịch vụ phổ biến bao gồm hạ tầng ảo (máy chủ EC2, máy ảo Azure...), dịch vụ lưu trữ (S3, Azure Blob Storage), cơ sở dữ liệu, phân tích dữ liệu lớn, v.v. Đám mây công cộng cung cấp tài nguyên theo yêu cầu với khả năng mở rộng linh hoạt và chi phí dựa trên mức sử dụng. Trong kiến trúc hybrid, phần workload có thể được triển khai trên public cloud để tận dụng những dịch vụ sẵn có và quy mô lớn của nhà cung cấp[[2]](https://developers.redhat.com/topics/hybrid-cloud-architecture#:~:text=Hybrid%20cloud%20setups%20have%20become,sensitivity%20and%20high%20volume%20requirements)[[6]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=A%20hybrid%20cloud%20model%20allows,as%20PaaS%20and%20IaaS%20services).
* **Mạng kết nối (Networking)**: Thành phần then chốt đảm bảo liên thông giữa môi trường tại chỗ và môi trường cloud. Kết nối này thường được thiết lập qua **mạng diện rộng (WAN)**, ví dụ Internet VPN hoặc đường truyền chuyên dụng (như AWS Direct Connect, Azure ExpressRoute) để đảm bảo băng thông và độ bảo mật cao. Mạng kết nối cần có độ trễ thấp và tin cậy, vì nhiều ứng dụng hybrid đòi hỏi trao đổi dữ liệu thời gian thực giữa on-premises và cloud. Các thiết bị mạng như firewall, router hỗ trợ VPN, cùng cấu hình mạng ảo trên cloud (VPC, Virtual Network) kết hợp tạo nên kênh truyền dẫn thống nhất[[22]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=Wide%20Area%20Networks%20,secure%20connection%20between%20two%20networks). Ngoài ra, cần thiết lập cơ chế DNS, cân bằng tải có thể hoạt động trên nhiều môi trường để người dùng truy cập dịch vụ một cách trong suốt dù backend nằm ở đâu.
* **Thành phần tích hợp và trung gian (Integration & Middleware)**: Đây là lớp phần mềm “keo nối” các môi trường lại với nhau. Bao gồm các API và dịch vụ tích hợp cho phép giao tiếp giữa ứng dụng chạy ở private và public cloud[[23]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=APIs%20are%20employed%20to%20facilitate,secure%20connection%20between%20two%20networks). Ví dụ, một ứng dụng có thể gọi API đến dịch vụ đám mây (như gọi AWS API Gateway hoặc Azure Functions) từ hệ thống nội bộ, hoặc ngược lại. Các **middleware** phổ biến trong hybrid cloud có thể là hệ thống nhắn tin (message queue) phân tán, dịch vụ đồng bộ dữ liệu, và đặc biệt là **API gateway** – cổng dịch vụ tập trung để các ứng dụng từ nhiều môi trường giao tiếp thông qua các API một cách thống nhất. API gateway có thể giúp thực thi chính sách an ninh, kiểm soát truy cập và chuyển đổi giao thức, đảm bảo các thành phần phân tán có thể hoạt động cùng nhau. Bên cạnh đó, nếu ứng dụng được kiến trúc dạng microservices, lớp tích hợp còn bao gồm **service mesh** để quản lý giao tiếp giữa các service trên nhiều cụm cloud khác nhau.
* **Lớp quản lý và điều phối (Management & Orchestration)**: Do hybrid cloud bao gồm nhiều môi trường, việc quản lý thủ công từng phần riêng lẻ là không hiệu quả. Thay vào đó, kiến trúc hybrid thường có lớp quản lý hợp nhất để giám sát, cấu hình và điều phối tài nguyên trên cả hai phía. Các **công cụ điều phối (orchestration)** cho phép triển khai ứng dụng đồng thời lên on-premises và cloud, tự động hóa các quy trình như khởi tạo máy ảo/container, cập nhật phiên bản, mở rộng hay thu hẹp tài nguyên. Ví dụ, Kubernetes hiện nay đóng vai trò quan trọng như một nền tảng điều phối container có thể chạy trên mọi môi trường, giúp quản trị cụm máy chủ lai một cách thống nhất. Nhiều nhà cung cấp cũng đưa ra giải pháp để quản lý hybrid: như **Azure Arc**, **Google Anthos**, **AWS Outposts**, cho phép quản lý tài nguyên on-premises bằng các dịch vụ cloud quen thuộc. Một báo cáo cho thấy các doanh nghiệp cần đầu tư vào các công cụ quản trị và điều phối tiên tiến để đảm bảo tích hợp trơn tru và an toàn cho hybrid cloud[[24]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=To%20mitigate%20these%20risks%2C%20enterprises,Cloud%20Security%20Alliance%2C%202019). Ngoài ra, lớp này cũng bao gồm quản lý cấu hình, giám sát hiệu năng, nhật ký, và các chính sách (policy) áp dụng đồng bộ.
* **Lớp bảo mật và danh tính (Security & Identity Management)**: An ninh phải bao trùm toàn bộ kiến trúc. Hệ thống hybrid thường triển khai các giải pháp quản lý danh tính tập trung (như tích hợp Active Directory/LDAP với dịch vụ cloud IAM) để đảm bảo người dùng có thể xác thực một lần và truy cập tài nguyên trên cả hai môi trường với quyền hạn thích hợp. Lớp bảo mật bao gồm mã hóa dữ liệu khi truyền qua mạng kết nối, tường lửa bảo vệ giữa các môi trường, hệ thống phát hiện và ngăn chặn xâm nhập, cũng như các giải pháp bảo vệ khối lượng công việc trên cloud (CWP). Việc duy trì **chính sách bảo mật nhất quán** giữa on-prem và cloud là thách thức, do đó các công cụ bảo mật hợp nhất hoặc dịch vụ bảo mật đám mây (như Cloud Security Posture Management) thường được đưa vào kiến trúc. Lớp này sẽ được bàn sâu hơn trong phần Bảo mật (mục 5).

Tất cả các thành phần trên hợp thành một kiến trúc hybrid cloud toàn diện. Mỗi tổ chức có thể có kiến trúc cụ thể khác nhau tùy thuộc vào việc họ sử dụng nhà cung cấp nào, khối lượng công việc ra sao, nhưng nhìn chung đều xoay quanh việc **kết hợp tài nguyên tại chỗ với tài nguyên đám mây công cộng** thông qua kết nối mạng an toàn và lớp phần mềm tích hợp, được quản lý bởi công cụ hợp nhất. Các thành phần cần được thiết kế sao cho khi ghép lại, hệ thống hoạt động như một **“đám mây duy nhất”** đối với người dùng cuối, dù thực chất các phần nằm ở các nơi khác nhau.

### 3.2. Mô hình triển khai Hybrid Cloud

Mô hình triển khai hybrid cloud có thể khác nhau tùy chiến lược và nhu cầu của doanh nghiệp, nhưng về cơ bản bao gồm sự kết hợp của **môi trường on-premise/private** và **môi trường cloud công cộng** cùng một kết nối an toàn giữa chúng. Hình 1 minh họa tổng quan về mô hình hybrid cloud, trong đó một phần ứng dụng và cơ sở dữ liệu chạy trên hạ tầng đám mây riêng/on-premise, phần còn lại chạy trên đám mây công cộng, tất cả tạo thành một môi trường lai thống nhất.

*Hình 1: Mô hình Hybrid Cloud kết hợp hạ tầng tại chỗ (private cloud, on-premises) với hạ tầng đám mây công cộng. Các ứng dụng on-premise, dịch vụ private cloud được liên kết với các dịch vụ public cloud thông qua mạng và các thành phần tích hợp, tạo thành một môi trường điện toán thống nhất.*

Trong triển khai thực tế, có một số kịch bản hybrid cloud phổ biến:

* **Mở rộng tải đột biến (Cloud Bursting)**: Đây là kịch bản cổ điển của hybrid cloud. Doanh nghiệp vận hành hệ thống chủ yếu trên hạ tầng riêng, nhưng khi lưu lượng hoặc nhu cầu tài nguyên tăng đột biến vượt quá năng lực nội bộ, workload sẽ được “đẩy” lên đám mây công cộng để mở rộng tạm thời[[3]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=NIST%27s%20original%20hybrid%20cloud%20definition,capacity%20wherever%20it%20was%20cheapest). Ví dụ, một ứng dụng web thương mại điện tử chạy trong datacenter của công ty, đến mùa mua sắm lượng truy cập tăng gấp nhiều lần, thay vì đầu tư thêm máy chủ chỉ phục vụ vài tuần cao điểm, hệ thống sẽ tự động khởi tạo thêm máy chủ ảo trên public cloud để gánh tải. Sau khi qua đỉnh, các máy chủ cloud có thể được tắt đi để tiết kiệm chi phí. Cloud bursting yêu cầu sự tương thích cao giữa hai môi trường và khả năng điều phối nhanh, đồng thời phải đảm bảo dữ liệu cần thiết được đồng bộ hoặc truy cập được từ môi trường cloud khi mở rộng.
* **Phân chia lớp ứng dụng**: Doanh nghiệp có thể triển khai một phần ứng dụng trên private cloud và phần khác trên public cloud dựa trên tính chất công việc. Một mô hình thường gặp là phần **frontend** (giao diện, ứng dụng web, mobile backend) đặt trên public cloud để tận dụng khả năng phục vụ người dùng toàn cầu và mở rộng linh hoạt, trong khi phần **backend** (cơ sở dữ liệu, hệ thống giao dịch chính) đặt ở private cloud nhằm bảo vệ dữ liệu nhạy cảm. Hai phần này giao tiếp qua mạng riêng bảo mật. Cách triển khai này phù hợp với các ứng dụng phân tầng, trong đó tầng giao tiếp không lưu trữ nhiều dữ liệu quan trọng có thể đưa lên cloud, còn dữ liệu được giữ an toàn trong nội bộ.
* **Phân theo môi trường phát triển**: Một số tổ chức sử dụng hybrid cloud để tách biệt môi trường phát triển/kiểm thử (development/testing) và môi trường sản xuất (production). Ví dụ: môi trường dev/test được tạo trên public cloud để các nhóm phát triển có thể nhanh chóng tạo máy chủ, thử nghiệm mà không ảnh hưởng hệ thống chính. Khi ứng dụng sẵn sàng, sẽ được triển khai trên hạ tầng private/ở chỗ để vận hành chính thức. Điều này tận dụng được tính linh hoạt và chi phí rẻ của cloud trong giai đoạn phát triển, đồng thời môi trường production vẫn duy trì trong tầm kiểm soát nội bộ[[25]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=,transformation%2C%20disaster%20recovery%20and%20development%2Ftesting).
* **Sao lưu và phục hồi thảm họa (Backup & Disaster Recovery)**: Hybrid cloud thường được sử dụng để xây dựng giải pháp DR. Dữ liệu từ hệ thống on-premise được sao lưu định kỳ lên cloud công cộng (sử dụng dịch vụ lưu trữ rẻ như Amazon S3, Glacier). Trong trường hợp trung tâm dữ liệu chính gặp sự cố (thiên tai, mất điện kéo dài), doanh nghiệp có thể kích hoạt hệ thống dự phòng trên cloud để tiếp tục cung cấp dịch vụ. Mô hình này tiết kiệm hơn việc duy trì một datacenter dự phòng vật lý thứ hai. Hybrid cloud đảm bảo tính liên tục kinh doanh nhờ hạ tầng cloud sẵn sàng gánh vác khi cần[[26]](https://developers.redhat.com/topics/hybrid-cloud-architecture#:~:text=Hybrid%20cloud%20systems%20also%20enable,for%20a%20fully%20private%20solution).
* **Xử lý dữ liệu lớn và phân tích (Big Data Analytics)**: Nhiều doanh nghiệp có dữ liệu lưu trữ tại chỗ (do yêu cầu bảo mật), nhưng khi cần thực hiện các tác vụ phân tích dữ liệu lớn hoặc machine learning đòi hỏi tài nguyên tính toán khổng lồ, họ có thể tận dụng các cụm máy chủ trên public cloud. Dữ liệu có thể được ẩn danh hoặc mã hóa rồi đưa tạm thời lên cloud để phân tích, sau đó kết quả trả về hệ thống nội bộ. Nhờ đó, doanh nghiệp khai thác được sức mạnh tính toán của cloud (ví dụ sử dụng hàng trăm nút xử lý song song) mà không phải đầu tư cụm máy chủ lớn tại chỗ vốn chỉ dùng ít khi[[27]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20benefits%20of%20hybrid%20cloud,based%20infrastructure)[[28]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Hybrid%20cloud%20computing%20has%20become,risk%20management%2C%20and%20data%20analytics). Cách tiếp cận này đặc biệt hữu ích trong các ngành như tài chính, khoa học, nơi khối lượng dữ liệu cực lớn nhưng yêu cầu tuân thủ cũng cao.
* **Triển khai đa cloud (Multi-cloud trong Hybrid)**: Một dạng triển khai phức tạp hơn là doanh nghiệp sử dụng nhiều nhà cung cấp cloud công cộng khác nhau cùng với hạ tầng on-premise, hình thành **hybrid multi-cloud**. Ví dụ, một công ty có datacenter riêng, đồng thời sử dụng cả AWS và Azure cho các phần việc khác nhau – AWS cho lưu trữ và máy chủ web, Azure cho dịch vụ AI. Các môi trường này được kết nối với nhau và có thể trao đổi qua lại. Mục tiêu có thể nhằm tránh phụ thuộc một nhà cung cấp duy nhất, tận dụng thế mạnh từng bên và tăng khả năng dự phòng khu vực. Theo chiến lược này, nhiều doanh nghiệp lớn (như HSBC) áp dụng cách tiếp cận *multi-cloud hybrid*, sử dụng đồng thời AWS, Azure, Google... kết hợp hệ thống nội bộ để đáp ứng yêu cầu vùng địa lý và tối ưu chi phí/nghiệp vụ[[29]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=The%20power%20of%20Cloud%20enables,vendor%20strengths%20and%20geographical%20coverage).

Mỗi mô hình triển khai hybrid nêu trên đều có những yêu cầu kỹ thuật cụ thể, nhưng tựu trung đều cần một kiến trúc vững chắc với kết nối mạng an toàn, cơ chế di chuyển dữ liệu và ứng dụng linh hoạt, cùng các chính sách rõ ràng về việc phần nào chạy ở đâu. Việc lựa chọn mô hình nào phụ thuộc vào mục tiêu sử dụng hybrid cloud của tổ chức: mở rộng tải, bảo vệ dữ liệu, tiết kiệm chi phí, hay tận dụng dịch vụ đặc thù từ cloud.

### 3.3. Các công nghệ hỗ trợ trong Hybrid Cloud

Để vận hành hiệu quả một kiến trúc hybrid cloud, nhiều công nghệ hiện đại đã và đang được sử dụng như những “viên gạch” xây dựng nên giải pháp. Dưới đây là một số công nghệ tiêu biểu hỗ trợ đắc lực cho mô hình hybrid:

* **Công nghệ ảo hóa và container**: Ảo hóa máy chủ là nền tảng của hầu hết các đám mây, cho phép tạo ra các máy ảo (VM) cách ly chạy trên cùng phần cứng. Trong hybrid cloud, doanh nghiệp có thể sử dụng cùng một nền tảng ảo hóa (VD: VMware vSphere) trên private cloud của mình tương tự như hạ tầng ảo hóa của public cloud, giúp việc di chuyển VM qua lại khả thi. Xa hơn, **container hóa** (Docker, Kubernetes) đang trở thành công nghệ không thể thiếu. Container giúp đóng gói ứng dụng và môi trường chạy một cách nhẹ và di động, làm mờ ranh giới giữa các môi trường triển khai. Nhờ Kubernetes – hệ thống điều phối container phổ biến – doanh nghiệp có thể triển khai một cụm (cluster) Kubernetes trải rộng trên cả on-premise và cloud, hoặc tích hợp các cluster riêng lẻ thành một môi trường logic thống nhất. Các hãng cung cấp như Red Hat OpenShift hay VMware Tanzu đã thương mại hóa những nền tảng dạng này, cho phép quản lý container đa đám mây thuận tiện. Tóm lại, container & Kubernetes mang lại **tính nhất quán (consistency)** và **di động (portability)** cao, giải quyết được một bài toán lớn của hybrid cloud trước đây[[7]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=The%20widespread%20adoption%20of%20containers,testing%2C%20and%20finally%20to%20production).
* **API và kiến trúc hướng dịch vụ**: Các hệ thống hybrid hiệu quả thường được xây dựng theo kiến trúc microservices hoặc hướng dịch vụ (SOA), trong đó các chức năng được tách thành dịch vụ nhỏ giao tiếp qua giao diện API rõ ràng. Điều này cho phép một số dịch vụ chạy on-premise, một số chạy trên cloud mà vẫn tương tác trơn tru. **API Gateway** là thành phần đóng vai trò cửa ngõ, xuất bản các API của hệ thống ra cho bên ngoài (hoặc cho các phần khác của hệ thống) sử dụng, đồng thời ẩn đi việc phía sau API đó là dịch vụ đang chạy ở đâu. Nhờ API gateway, việc chuyển một dịch vụ từ on-prem lên cloud hoặc ngược lại có thể không ảnh hưởng tới các thành phần khác nếu URL và hợp đồng API không đổi. Ngoài ra, các **giao thức tích hợp** như messaging (RabbitMQ, Kafka) hay event streaming cũng thường được dùng để nối kết thành phần phân tán. Ví dụ, một hàng đợi tin nhắn có thể được đặt ở cả hai môi trường, cho phép ứng dụng ở private gửi thông điệp và ứng dụng ở public nhận và xử lý sau vài giây, đảm bảo liên tục quy trình nghiệp vụ.
* **Mạng và kết nối an toàn**: Công nghệ mạng hỗ trợ hybrid cloud bao gồm **VPN (Virtual Private Network)**, **SD-WAN** và các kết nối chuyên dụng. VPN mã hóa kết nối Internet giữa datacenter và cloud tạo thành một mạng riêng ảo, giúp hai môi trường giao tiếp như trong một mạng nội bộ an toàn[[23]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=APIs%20are%20employed%20to%20facilitate,secure%20connection%20between%20two%20networks). SD-WAN cho phép định tuyến thông minh lưu lượng qua nhiều liên kết, tối ưu đường truyền cho ứng dụng quan trọng. Ngoài ra, các nhà cung cấp cloud có dịch vụ kết nối riêng (ví dụ AWS Direct Connect, Azure ExpressRoute) cho phép doanh nghiệp thuê kênh truyền trực tiếp đến hạ tầng cloud, giảm độ trễ và tăng bảo mật (dữ liệu không đi qua Internet công cộng). Công nghệ **mạng ảo đám mây** (Virtual VPC/VNet) cho phép cấu hình mạng trên cloud tương thích với mạng on-prem (địa chỉ IP, subnet), tạo cảm giác một mạng duy nhất. Những tiến bộ trong mạng như vậy rất quan trọng để hybrid cloud hoạt động với hiệu năng và độ an toàn cao.
* **Công cụ quản lý đa đám mây và hạ tầng dưới dạng mã (IaC)**: Khi vận hành hybrid cloud, doanh nghiệp thường sử dụng các công cụ quản lý đa đám mây để theo dõi tài nguyên, chi phí và hiệu suất trên nhiều môi trường. Các giải pháp từ bên thứ ba hoặc của chính nhà cung cấp (như Azure Arc, Google Cloud Management) giúp hợp nhất việc quản lý. Đồng thời, việc triển khai hạ tầng bằng mã (Infrastructure as Code - IaC) ngày càng thông dụng. Các công cụ như Terraform, Ansible, CloudFormation cho phép định nghĩa tài nguyên (máy chủ, mạng, dịch vụ) bằng mã hoặc kịch bản, và áp dụng lên cả môi trường on-prem lẫn cloud. Nhờ IaC, cấu hình của các môi trường có thể được giữ tương đồng và dễ dàng tái tạo, giảm lỗi cấu hình thủ công – vốn là nguyên nhân gây nhiều sự cố an ninh trên cloud[[30]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Another%20significant%20risk%20is%20the,regularly%20updated%20to%20prevent%20vulnerabilities). IaC cũng giúp tự động hóa việc mở rộng, triển khai, góp phần hiện thực hóa khả năng linh hoạt của hybrid cloud.
* **Orchestration & Automation (Điều phối và tự động hóa)**: Như đã đề cập, một thách thức của hybrid cloud là quản lý tính phức tạp. Do đó, các nền tảng điều phối được sử dụng để tự động hóa hầu hết các tác vụ quản trị. Ngoài Kubernetes cho container, còn có các bộ điều phối khác cho hạ tầng ảo (như VMware vRealize cho hybrid cloud), hoặc các dịch vụ orchestration đi kèm cloud (AWS OpsWorks, Google Cloud Composer). Mục tiêu là đạt được khả năng triển khai ứng dụng mới, áp dụng bản vá, thay đổi cấu hình một cách tự động trên phạm vi rộng mà không cần thao tác thủ công tẻ nhạt trên từng môi trường. Các kịch bản CI/CD (tích hợp liên tục và triển khai liên tục) cũng được mở rộng sang hybrid: ví dụ pipeline CI/CD có thể triển khai ứng dụng lên cả cụm on-prem và cụm cloud cùng lúc. Một khảo sát cho thấy 60% tổ chức gặp khó khăn trong việc quản lý nhiều nhà cung cấp cloud, dẫn đến tăng độ phức tạp và chi phí[[31]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=However%2C%20implementing%20hybrid%20clouds%20also,of%20security%20and%20compliance%20standards). Điều này nhấn mạnh tầm quan trọng của automation – chỉ khi tự động hóa tốt, doanh nghiệp mới thực sự khai thác hiệu quả hybrid cloud mà không bị quá tải bởi công việc quản trị.
* **Các công nghệ khác**: Bên cạnh những công nghệ chủ lực trên, còn nhiều công cụ và phương pháp hỗ trợ hybrid cloud. Chẳng hạn: **giám sát phân tán** (distributed tracing, APM) để theo dõi giao dịch trải qua nhiều môi trường; **Data virtualization** cho phép truy cập dữ liệu thống nhất dù dữ liệu nằm rải rác (giúp ứng dụng không cần biết chính xác dữ liệu ở cloud hay on-prem); **Edge computing** kết hợp với hybrid cloud để đưa một phần xử lý xuống gần nguồn dữ liệu (thiết bị biên) trong khi vẫn kết nối với cloud trung tâm. Ngoài ra, các tiêu chuẩn mở về tương thích cloud (như OpenStack cho private, hoặc Kubernetes như một “layer chung”) cũng giúp giảm hiện tượng khóa nhà cung cấp, tạo điều kiện cho hybrid cloud linh hoạt hơn.

Tóm lại, sự phát triển của hàng loạt công nghệ từ ảo hóa, container, mạng đến phần mềm quản trị đã tạo tiền đề để hybrid cloud trở thành hiện thực. Nếu không có chúng, việc kết hợp hai thế giới on-premise và cloud sẽ vô cùng khó khăn. Việc lựa chọn và áp dụng đúng các công nghệ phù hợp sẽ quyết định thành công của một dự án hybrid cloud, giúp hệ thống vận hành trơn tru, bảo mật và đạt được mục tiêu kinh doanh đề ra.

## 4. Ứng dụng thực tế trong doanh nghiệp

### 4.1. Các kịch bản sử dụng Hybrid Cloud

Hybrid cloud hiện diện trong nhiều kịch bản ứng dụng doanh nghiệp, từ những nhu cầu CNTT thông thường đến các bài toán đặc thù. Dưới đây là một số ví dụ về cách doanh nghiệp tận dụng hybrid cloud trong thực tế:

* **Lưu trữ dữ liệu và chia sẻ tải**: Doanh nghiệp có thể sử dụng hybrid cloud để lưu trữ các bộ dữ liệu lớn. Dữ liệu nhạy cảm (như thông tin khách hàng, tài chính) được lưu trên hạ tầng riêng để đảm bảo tuân thủ quy định (ví dụ dữ liệu khách hàng châu Âu lưu trong datacenter nội bộ để tuân thủ GDPR). Trong khi đó, các dữ liệu ít nhạy cảm hơn hoặc dữ liệu sao lưu, lưu trữ lâu dài được đưa lên đám mây công cộng (nhờ chi phí rẻ và khả năng mở rộng). Khi cần phân tích trên toàn bộ dữ liệu, hệ thống có thể tạm thời kết hợp hai nguồn lại. Cách làm này vừa tối ưu chi phí lưu trữ, vừa đảm bảo yêu cầu địa phương hóa dữ liệu. Một ví dụ khác: ứng dụng chia sẻ tệp trong doanh nghiệp có thể giữ bản chính trên server nội bộ, đồng thời sử dụng dịch vụ cloud để phân phối file đến các chi nhánh xa qua CDN, tăng tốc độ truy cập mà vẫn kiểm soát được bản nguồn.
* **Phân tích Big Data và ML linh hoạt**: Như đã đề cập, phân tích dữ liệu lớn hưởng lợi nhiều từ hybrid cloud. Một công ty bán lẻ có thể giữ dữ liệu giao dịch trên hệ thống tại chỗ (do tích hợp với hệ thống POS, ERP cũ), nhưng định kỳ đẩy dữ liệu bán hàng lên cloud để chạy thuật toán phân tích thị trường hoặc huấn luyện mô hình học máy (machine learning) nhằm dự báo nhu cầu. Cloud cung cấp tài nguyên GPU, TPU mạnh mẽ mà công ty không sở hữu. Sau khi có kết quả (ví dụ các xu hướng mua sắm), kết quả được nhập về hệ thống nội bộ để các quản lý sử dụng. Toàn bộ quá trình có thể tự động: hàng đêm, dữ liệu được đồng bộ lên cloud, xử lý, rồi trả kết quả. Các công ty trong lĩnh vực tài chính, bảo hiểm cũng dùng mô hình tương tự cho các tính toán rủi ro phức tạp: hệ thống core chạy tại chỗ, nhưng mỗi cuối ngày sẽ copy snapshot dữ liệu lên cloud để chạy tính toán, sáng hôm sau nhập kết quả lại.
* **Web ứng dụng và dịch vụ linh hoạt**: Đối với các dịch vụ trực tuyến (web service, mobile backend), hybrid cloud cung cấp sự linh hoạt để ứng phó các tình huống biến động. Ví dụ, một công ty trò chơi trực tuyến đặt máy chủ game chính ở datacenter riêng để có độ trễ thấp cho người dùng nội địa. Nhưng khi có sự kiện toàn cầu hoặc lượng người chơi tăng đột biến, công ty có thể triển khai thêm server game trên cloud ở nhiều khu vực khác để giảm tải cho server chính. Tương tự, các trang web thương mại hay tin tức khi có chiến dịch marketing lớn, thay vì nâng cấp hạ tầng trong nước, họ có thể thuê thêm tài nguyên cloud tạm thời để đảm bảo website không sập khi lượng truy cập tăng vọt (đây cũng là dạng cloud bursting). Sau chiến dịch, các tài nguyên cloud được giải phóng để tiết kiệm chi phí.
* **Môi trường phát triển, thử nghiệm (Dev/Test)**: Nhiều doanh nghiệp ứng dụng hybrid cloud để tăng tốc phát triển phần mềm. Thay vì chờ cấp máy chủ trong nội bộ – vốn có thể mất vài tuần để mua sắm/cài đặt – các kỹ sư có thể tự động tạo môi trường thử nghiệm trên cloud chỉ trong vài giờ. Môi trường này mô phỏng tương tự như môi trường thật (về hệ điều hành, middleware) nhưng chạy tạm trên cloud. Khi thử nghiệm xong, môi trường có thể xóa đi. Cách làm này tăng hiệu suất làm việc, đồng thời giảm gánh nặng lên hạ tầng nội bộ. Một ví dụ: ngân hàng HSBC áp dụng phương pháp DevOps kết hợp đám mây, cho phép các nhóm phát triển sử dụng mindset “fail fast” – thử nghiệm nhanh trên cloud, tự động hóa triển khai, sau đó khi dịch vụ ổn định mới triển khai về môi trường chính thức được kiểm soát chặt chẽ[[32]](https://cloud.google.com/customers/featured/hsbc#:~:text=HSBC%20Customer%20Hub%20,automation%20built%20in%20along)[[29]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=The%20power%20of%20Cloud%20enables,vendor%20strengths%20and%20geographical%20coverage). Điều này cho phép ngân hàng đổi mới nhanh hơn nhưng vẫn đảm bảo an toàn cho hệ thống cốt lõi.
* **Đảm bảo tính sẵn sàng cao và khôi phục sau thảm họa**: Một kịch bản khác là sử dụng hybrid cloud để tăng tính sẵn sàng (HA) cho ứng dụng. Ví dụ, một hệ thống giao dịch chứng khoán có trung tâm dữ liệu chính ở Hà Nội, trung tâm dữ liệu dự phòng ở TP. Hồ Chí Minh. Ngoài ra, để tăng cường, công ty thiết lập thêm một cụm máy chủ trên cloud (ví dụ Google Cloud region ở Singapore) làm site thứ ba. Dữ liệu được sao chép thời gian thực sang cụm cloud này. Nếu cả hai site vật lý gặp sự cố (giả sử do sự kiện mất điện diện rộng), site cloud có thể tiếp quản tạm thời để duy trì dịch vụ liên tục. Hoặc ngay cả khi không cần chuyển hoàn toàn, site cloud có thể giúp san tải (load sharing) trong giờ cao điểm, giảm gánh nặng cho hệ thống chính. Nhờ sự linh hoạt của cloud, doanh nghiệp có thể thiết lập mô hình *Active-Active* đa site với chi phí chấp nhận được (vì tài nguyên cloud có thể điều chỉnh theo nhu cầu, không như đầu tư cứng cho site vật lý).

Những kịch bản trên cho thấy hybrid cloud không chỉ là khái niệm lý thuyết mà đã và đang giải quyết nhiều bài toán thực tế. Theo một khảo sát của IDG, top các lý do doanh nghiệp lựa chọn hybrid cloud bao gồm: tăng **sự linh hoạt trong kinh doanh**, tiết kiệm **chi phí**, và cải thiện **bảo mật** so với chỉ dùng public cloud đơn thuần[[33]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20adoption%20rate%20of%20hybrid,effectiveness%20in%20enterprise%20IT%20environments)[[34]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=effectiveness%20in%20enterprise%20IT%20environments). Điều này phản ánh qua các trường hợp sử dụng: doanh nghiệp có thể phản ứng nhanh với thay đổi thị trường, mở rộng hoặc co hẹp hệ thống tùy nhu cầu (business agility); chỉ phải trả tiền cho tài nguyên cloud khi dùng thay vì duy trì dư thừa (cost saving); và giữ được những gì quan trọng trong tầm tay kiểm soát (security).

### 4.2. Case study từ các doanh nghiệp lớn

Rất nhiều tập đoàn lớn trên thế giới đã triển khai thành công mô hình hybrid cloud, cho thấy tính hiệu quả và linh hoạt của kiến trúc này. Sau đây là một số **case study tiêu biểu** từ các lĩnh vực khác nhau:

* **Netflix (Truyền thông & Giải trí)**: Netflix – dịch vụ streaming hàng đầu thế giới – nổi tiếng với việc tận dụng triệt để sức mạnh của điện toán đám mây. Netflix đã chuyển toàn bộ hệ thống của mình sang chạy trên **Amazon Web Services (AWS)**, biến nó thành một ví dụ điển hình về khả năng mở rộng vô hạn của cloud. Nhờ AWS, Netflix có thể nhanh chóng triển khai hàng ngàn máy chủ và hàng petabyte lưu trữ chỉ trong vài phút để phục vụ người xem khắp toàn cầu[[35]](https://aws.amazon.com/solutions/case-studies/netflix-case-study/#:~:text=Online%20content%20provider%20Netflix%20can,mobile%20devices%20such%20as%20iPhones). Mỗi ngày, Netflix cung cấp hàng tỷ giờ nội dung cho hơn 200 triệu thuê bao, và toàn bộ hạ tầng backend cùng hệ thống phân tích dữ liệu của họ đều chạy trên cloud[[36]](https://aws.amazon.com/solutions/case-studies/netflix-case-study/#:~:text=Netflix%20Delivers%20Billions%20of%20Hours,Globally%20by%20Running%20on%20AWS). Mặc dù Netflix chủ yếu dựa vào public cloud (thực tế họ không duy trì data center riêng), trường hợp này cho thấy lợi ích mà hybrid hoặc public cloud mang lại về quy mô và độ sẵn sàng. Ngoài ra, Netflix còn phát triển mạng lưới CDN riêng gọi là **Netflix Open Connect** – triển khai các máy chủ lưu trữ nội dung tại ISP địa phương – kết hợp với hạ tầng AWS để tăng chất lượng streaming. Đây có thể xem như một dạng kiến trúc lai đặc thù: phần phân phối nội dung do Netflix kiểm soát (thông qua các máy chủ Open Connect đặt bên ngoài AWS), trong khi phần quản lý và xử lý chính chạy trên AWS. Chiến lược này giúp Netflix tối ưu trải nghiệm người dùng đồng thời tận dụng hạ tầng cloud cho phần linh hoạt.
* **BMW (Sản xuất ô tô)**: Tập đoàn BMW đã thực hiện hành trình chuyển đổi số mạnh mẽ với chiến lược hybrid multi-cloud. BMW sử dụng đồng thời nhiều nhà cung cấp đám mây công cộng bao gồm **Microsoft Azure và AWS**, kết hợp với hệ thống CNTT nội bộ, nhằm xây dựng một nền tảng đám mây phục vụ toàn cầu. Thách thức đặt ra là làm sao quản lý thống nhất hạ tầng đa dạng này khi quy mô và số lượng dịch vụ cloud tăng nhanh. Để giải quyết, BMW hợp tác với công ty Nordcloud để phát triển một **Public Cloud Platform** – cổng quản lý trung tâm cho phép các đội ngũ trong BMW truy cập dịch vụ cloud một cách tuân thủ và hiệu quả[[37]](https://nordcloud.com/case-studies/bmw-group/#:~:text=The%20client)[[38]](https://nordcloud.com/case-studies/bmw-group/#:~:text=The%20BMW%20Group%20wanted%20a,both%20Microsoft%20Azure%20and%20AWS). Nền tảng này thiết lập các cấu hình chuẩn, quy trình tự động để các nhóm có thể yêu cầu tài nguyên trên Azure hoặc AWS nhanh chóng mà vẫn đảm bảo tuân thủ quy định an ninh của tập đoàn. Kết quả, BMW tăng tốc độ cung cấp môi trường cloud lên 50%, tự động hóa hàng chục nghìn yêu cầu dịch vụ, và quản lý tập trung tài nguyên đa cloud trên phạm vi toàn cầu[[39]](https://nordcloud.com/case-studies/bmw-group/#:~:text=%2A%2050,and%20management%20of%20cloud%20resources)[[40]](https://nordcloud.com/case-studies/bmw-group/#:~:text=Multi). Trường hợp BMW cho thấy một doanh nghiệp sản xuất truyền thống có thể tận dụng hybrid cloud (ở đây bao gồm on-premise và multi-cloud) để hỗ trợ đổi mới sáng tạo, từ việc phát triển xe tự lái (cần sức mạnh tính toán lớn) cho đến cung cấp dịch vụ kỹ thuật số cho khách hàng xe hơi trên toàn thế giới. Sự kết hợp Azure-AWS-onPrem cũng giúp BMW tránh phụ thuộc duy nhất vào một hạ tầng, tăng tính linh hoạt trong lựa chọn công nghệ tối ưu cho từng tác vụ.
* **HSBC (Dịch vụ tài chính – ngân hàng)**: HSBC là một trong những tổ chức tài chính lớn nhất toàn cầu, hoạt động ở hơn 60 quốc gia. Trong lĩnh vực ngân hàng, yêu cầu về bảo mật và tuân thủ rất cao, do đó HSBC không thể đưa tất cả dữ liệu và hệ thống lên public cloud một cách tùy tiện. Thay vào đó, HSBC áp dụng chiến lược **đa đám mây (multi-cloud)** kết hợp với hạ tầng truyền thống, nhằm cân bằng giữa đổi mới và kiểm soát. Theo CTO phụ trách dịch vụ đám mây của HSBC, ngân hàng này sử dụng công nghệ của nhiều hãng bao gồm **Google, Amazon, Microsoft và cả Alibaba Cloud**[[29]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=The%20power%20of%20Cloud%20enables,vendor%20strengths%20and%20geographical%20coverage). Cách tiếp cận multi-cloud giúp HSBC tận dụng được thế mạnh từng nhà cung cấp (ví dụ: Google Cloud cho phân tích dữ liệu với AI/ML, AWS cho quy mô và hệ sinh thái phong phú, Azure cho tích hợp với giải pháp doanh nghiệp Microsoft) đồng thời tránh bị khóa chặt vào một nhà cung cấp – một điều quan trọng cho chiến lược thoát hiểm và thương thảo giá tốt hơn[[41]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=industry%20leading%20technology%20from%20Google%2C,vendor%20strengths%20and%20geographical%20coverage). HSBC triển khai các ứng dụng mới trên cloud để tăng tốc độ ra dịch vụ cho khách hàng (chẳng hạn ứng dụng mobile banking **Kinetic** ở Anh được xây dựng hoàn toàn trên cloud)[[42]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=means%20that%20we%20can%20create,flow%20forecasting%20and%20business%20insights). Tuy nhiên, họ vẫn duy trì các hệ thống core banking quan trọng trên mainframe và private cloud nội bộ, kết nối với các dịch vụ cloud qua các lớp API an toàn. Việc *“đưa ngân hàng lên mây”* giúp HSBC cải thiện đáng kể khả năng mở rộng, khi những quy trình trước đây mất hàng tuần thì nay có thể hoàn tất trong vài phút[[43]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=Ultimately%20our%20use%20of%20Cloud,Users%20benefit%20from%20account). Đồng thời, việc sử dụng hybrid cloud còn hỗ trợ HSBC trong mục tiêu phát triển bền vững: họ nhận thấy việc chuyển một phần workload lên cloud giúp giảm lượng khí thải carbon do tận dụng hiệu quả hạ tầng và năng lượng tái tạo của các cloud provider, góp phần vào cam kết trung hòa carbon của ngân hàng[[44]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=Cloud%20efficiency%20is%20particularly%20important,chain%20by%202030%20or%20sooner)[[45]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=Our%20Cloud%20providers%20share%20our,Cloud%20we%20use%20zero%20energy). Trải nghiệm của HSBC cho thấy ngay cả ngành bảo thủ như ngân hàng cũng đang dần “cloud-first” thông qua con đường hybrid, giữ các thành phần nhạy cảm trong vùng an toàn nhưng vẫn khai thác công nghệ mới trên cloud để không bị tụt hậu.
* **Walmart (Bán lẻ)**: Walmart, tập đoàn bán lẻ lớn nhất thế giới, đã xây dựng một kiến trúc hybrid cloud để tối ưu chuỗi cung ứng và trải nghiệm khách hàng. Walmart vận hành hàng loạt hệ thống on-premise trong các trung tâm dữ liệu riêng phục vụ cho cửa hàng và thương mại điện tử. Song song, họ kết hợp sử dụng dịch vụ cloud từ nhiều nhà cung cấp. Một ví dụ, Walmart triển khai kiến trúc lai kết hợp hạ tầng tại chỗ với dịch vụ từ **Microsoft Azure và AWS**[[46]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=One%20notable%20example%20of%20successful,customer%20experience%2C%20and%20reduce%20costs). Mục tiêu là cải thiện quản lý chuỗi cung ứng: dữ liệu bán hàng từ cửa hàng có thể được đưa lên cloud để phân tích thời gian thực, từ đó tối ưu tồn kho và logistics. Đồng thời, ứng dụng di động và website thương mại điện tử của Walmart được host trên cloud để đảm bảo khả năng phục vụ hàng triệu khách mua sắm trực tuyến, đặc biệt trong các dịp cao điểm như Black Friday. Kết quả là Walmart đã nâng cao hiệu quả vận hành và trải nghiệm khách hàng, đồng thời cắt giảm chi phí cơ sở hạ tầng nhờ chỉ phải mở rộng khi cần thiết trên cloud[[47]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=architecture%20that%20combines%20on,customer%20experience%2C%20and%20reduce%20costs)[[48]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20use%20of%20hybrid%20cloud,customer%20experience%2C%20and%20reduce%20costs). Trường hợp Walmart minh họa cho việc một doanh nghiệp bán lẻ truyền thống có thể chuyển mình với hybrid cloud, kết hợp dữ liệu từ cửa hàng vật lý và sức mạnh tính toán của cloud để xây dựng hệ thống bán lẻ thông minh.
* **JPMorgan Chase (Tài chính)**: JPMorgan Chase, một trong những ngân hàng đầu tư lớn nhất tại Mỹ, cũng áp dụng hybrid cloud để cân bằng giữa đổi mới và an toàn. Họ duy trì các trung tâm dữ liệu riêng cho các hệ thống giao dịch nhạy cảm, nhưng đồng thời sử dụng đám mây công cộng (cụ thể là AWS) cho một số tác vụ phân tích rủi ro và dịch vụ khách hàng kỹ thuật số. JPMorgan đã triển khai hạ tầng hybrid kết hợp on-premises với AWS, giúp ngân hàng này cải thiện năng lực quản lý rủi ro (nhờ có thể chạy các mô phỏng phức tạp trên hàng ngàn máy chủ AWS), nâng cao trải nghiệm khách hàng (các dịch vụ ngân hàng trực tuyến hoạt động mượt mà hơn), đồng thời tối ưu chi phí vận hành[[49]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Another%20example%20is%20the%20use,customer%20experience%2C%20and%20reduce%20costs). Do lĩnh vực tài chính chịu sự giám sát nghiêm ngặt, JPMorgan chú trọng xây dựng các *guardrail* (lan can an toàn) khi dùng cloud, ví dụ mã hóa mạnh, kiểm soát truy cập nghiêm ngặt và giám sát liên tục để đảm bảo không có dữ liệu nhạy cảm nào bị phơi ra. Thành công của JPMorgan với hybrid cloud khẳng định mô hình này khả thi ngay cả khi yêu cầu an ninh cao.

Các case study trên, từ công ty công nghệ số (Netflix) cho đến hãng sản xuất, ngân hàng, bán lẻ, đã chứng minh tính linh hoạt và hiệu quả của hybrid cloud. Theo dự báo, xu hướng này sẽ tiếp tục tăng: thị trường hybrid cloud toàn cầu được dự đoán tăng từ 43 tỷ USD năm 2020 lên khoảng 157-162 tỷ USD vào năm 2025[[50]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=According%20to%20a%20study%20by,IDG%2C%202022)[[51]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20adoption%20of%20hybrid%20cloud,sized%20businesses). Hầu hết các tổ chức lớn đều đang trong lộ trình áp dụng chiến lược hybrid hoặc multi-cloud để không bỏ lỡ cơ hội từ điện toán đám mây, đồng thời bảo vệ các tài sản quan trọng và duy trì tính tuân thủ.

## 5. Bảo mật và tuân thủ

### 5.1. Rủi ro bảo mật trong mô hình Hybrid Cloud

Mô hình hybrid cloud, dù mang lại nhiều lợi ích, cũng đồng thời mở ra **những thách thức mới về bảo mật**. Việc kết hợp nhiều môi trường – mỗi môi trường có cơ chế bảo mật riêng – tạo ra một bề mặt tấn công (attack surface) rộng hơn, phức tạp hơn so với việc quản lý hạ tầng tập trung. Sau đây là một số rủi ro bảo mật chính trong hybrid cloud:

* **Tấn công truy cập trái phép (Unauthorized Access)**: Do hệ thống hybrid có kết nối ra bên ngoài (đến đám mây công cộng), nguy cơ bị truy cập trái phép tăng lên nếu kiểm soát không chặt. Theo Gartner, có tới 60% tổ chức đã trải qua sự cố bảo mật liên quan đến cloud trong năm 2022[[52]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=One%20of%20the%20primary%20concerns,in%20transit%20and%20at%20rest). Kẻ tấn công có thể tìm cách xâm nhập thông qua các API dịch vụ cloud nếu thông tin xác thực (credentials) bị lộ hoặc cấu hình sai. Việc quản lý tài khoản, phân quyền trên môi trường cloud đôi khi không đồng bộ với chính sách nội bộ, dẫn đến lỗ hổng (ví dụ: một tài khoản cloud vô tình được quyền truy cập dữ liệu nhạy cảm). Ngoài ra, nếu kẻ tấn công xâm nhập được môi trường on-premise (qua lỗ hổng mạng nội bộ) thì có thể lợi dụng kết nối hybrid để lần ra tới các tài nguyên trên cloud và ngược lại. Tóm lại, sự đan xen các môi trường đòi hỏi phải giám sát nghiêm ngặt hơn danh tính và quyền truy cập.
* **Cấu hình sai và lỗ hổng cấu hình (Misconfiguration)**: Đây được xem là rủi ro hàng đầu trong môi trường đám mây. Một báo cáo của IBM cho thấy 95% tổ chức bị vi phạm dữ liệu trên cloud năm 2022, và nhiều sự cố là do cấu hình sai cấu phần cloud[[30]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Another%20significant%20risk%20is%20the,regularly%20updated%20to%20prevent%20vulnerabilities). Ví dụ điển hình: cấu hình lưu trữ S3 bucket trên AWS ở chế độ công khai khiến dữ liệu nội bộ bị lộ ra internet, hoặc lỗ hổng do quên bật mã hóa cho một cơ sở dữ liệu cloud. Trong hybrid cloud, rủi ro này nhân lên khi quản trị viên phải cấu hình nhiều môi trường khác nhau với công cụ khác nhau – chỉ một sơ suất nhỏ cũng có thể mở cửa cho tấn công. Việc đảm bảo **cấu hình an toàn đồng nhất** giữa on-premise và cloud là thách thức, vì mỗi bên có tập thông số riêng (như group policy nội bộ vs. security group trên AWS). Nếu không có quy trình quản lý cấu hình và kiểm tra thường xuyên, dễ có chỗ sót dẫn đến lỗ hổng.
* **Rủi ro về dữ liệu**: Dữ liệu di chuyển qua lại giữa private và public cloud có nguy cơ bị chặn thu (eavesdrop) hoặc bị lưu trữ ở nơi không an toàn. Chẳng hạn, nếu kết nối VPN không được mã hóa mạnh, kẻ tấn công có thể nghe lén lưu lượng trên đường truyền. Hoặc khi chuyển dữ liệu từ on-prem lên cloud để xử lý, có khả năng bản sao dữ liệu đó nằm trên hạ tầng cloud (ổ đĩa tạm, snapshot) và nếu không xóa kỹ, dữ liệu nhạy cảm có thể tồn tại ngoài tầm kiểm soát. Ngoài ra, việc **định vị dữ liệu (data residency)** cũng là một vấn đề bảo mật/tuân thủ: thông tin cá nhân của người dùng có thể vô tình bị chuyển sang lưu trữ ở quốc gia khác khi sử dụng cloud, vi phạm quy định (ví dụ GDPR yêu cầu dữ liệu công dân EU phải ở trong EU). Sự phức tạp trong quản lý vị trí và vòng đời dữ liệu trên hybrid cloud làm tăng nguy cơ vi phạm bảo mật dữ liệu.
* **Tấn công vào API và dịch vụ**: Hybrid cloud hoạt động dựa nhiều vào các API (ví dụ API của AWS/Azure, API của các dịch vụ nội bộ). Các API này trở thành mục tiêu hấp dẫn cho hacker. Tấn công injection, DoS, hay khai thác lỗ hổng logic API có thể làm rò rỉ dữ liệu hoặc giành quyền điều khiển dịch vụ. Nếu một API gateway trung tâm bị tấn công, kẻ xấu có thể chuyển hướng hoặc nghe lén lưu lượng giữa các thành phần hybrid. Môi trường cloud thường công khai một số endpoint dịch vụ (ví dụ endpoint để gọi chức năng serverless), nếu hacker tìm ra và khai thác lỗ hổng trong việc xác thực đầu cuối, họ có thể giả mạo các yêu cầu từ nội bộ.
* **Quản lý danh tính và truy cập (IAM) phức tạp**: Nghiên cứu của Forrester cho thấy 70% tổ chức gặp khó khăn với quản lý danh tính trong môi trường cloud[[53]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=In%20addition%20to%20these%20risks%2C,demands%20of%20hybrid%20cloud%20environments). Trong hybrid cloud, doanh nghiệp phải quản lý người dùng nội bộ (thường qua AD/LDAP) lẫn người dùng trên cloud IAM (như tài khoản IAM của AWS, Azure AD). Nếu hai hệ thống này không được liên kết, việc thu hồi quyền truy cập khi nhân viên nghỉ việc hoặc thay đổi vai trò có thể bị bỏ sót trên một trong hai môi trường. Ngoài ra, việc thiết lập cơ chế xác thực đa yếu tố (MFA) đồng bộ trên cả on-prem và cloud là bắt buộc nhưng đôi khi bị lơ là trên cloud do triển khai vội. Sự không đồng bộ IAM có thể tạo lỗ hổng – ví dụ hacker tấn công tài khoản cloud vì biết tài khoản đó không có MFA dù tài khoản nội bộ thì có.
* **Tấn công DoS phân tán**: Cloud cho phép mở rộng linh hoạt nhưng cũng có thể bị lạm dụng bởi tấn công từ chối dịch vụ. Một kẻ tấn công có thể cố tình gửi lượng lớn traffic vào cổng kết nối giữa on-prem và cloud, làm nghẽn băng thông VPN khiến hai môi trường mất liên lạc, làm gián đoạn dịch vụ. Hoặc tấn công DDoS nhắm vào ứng dụng đang chạy trên public cloud trong mô hình hybrid; nếu không có biện pháp như auto-scaling hoặc dịch vụ chặn DDoS của nhà cung cấp, phần hybrid trên cloud có thể bị đánh sập, kéo theo ảnh hưởng đến toàn hệ thống.
* **Môi trường phát triển/test trên cloud kém an toàn**: Nhiều doanh nghiệp triển khai dev/test trên cloud nhưng không tuân thủ các chính sách bảo mật nghiêm ngặt như môi trường production. Hacker có thể tập trung tấn công môi trường này – thường dễ xâm nhập hơn – rồi từ đó lần ra bí mật (như khóa API, thông tin hạ tầng) để tấn công môi trường chính. Đã có trường hợp thông tin xác thực quản trị cloud bị để trong mã nguồn test và hacker tìm thấy, từ đó chiếm quyền trên toàn bộ tài khoản cloud. Do đó, dev/test trên cloud cũng phải được bảo vệ tương tự production, nhưng thực tế không phải lúc nào cũng vậy.

Tóm lại, hybrid cloud đem đến **bề mặt tấn công rộng và đa dạng** hơn, từ mạng, ứng dụng đến con người. Theo Cloud Security Alliance, việc đảm bảo an ninh trên hybrid cloud đòi hỏi cách tiếp cận nhiều lớp và nhất quán, nếu không các lỗ hổng từ mỗi bên có thể cộng hưởng với nhau[[31]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=However%2C%20implementing%20hybrid%20clouds%20also,of%20security%20and%20compliance%20standards)[[54]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20hybrid%20cloud%20market%20is,in%20%2844). Nhận thức được các rủi ro nêu trên là bước đầu để doanh nghiệp xây dựng các biện pháp phòng thủ phù hợp.

### 5.2. Giải pháp đảm bảo an ninh và quản lý dữ liệu

Để khắc phục các rủi ro kể trên, doanh nghiệp cần triển khai một loạt **giải pháp bảo mật tích hợp** phù hợp với mô hình hybrid. Dưới đây là các hướng chính để đảm bảo an ninh và quản lý dữ liệu hiệu quả trong môi trường đám mây lai:

* **Kiểm soát truy cập chặt chẽ (Strengthened Access Control)**: Điều này bao gồm áp dụng mô hình **Zero Trust** – luôn xác minh mỗi yêu cầu truy cập bất kể đến từ mạng nội bộ hay bên ngoài. Cụ thể, cần tích hợp hệ thống quản lý danh tính (IAM) giữa on-prem và cloud. Một giải pháp thường dùng là thiết lập **liên kết danh tính (federation)**: ví dụ, cho phép dùng tài khoản Active Directory nội bộ để đăng nhập vào tài nguyên AWS/Azure, nhờ đó khi một nhân sự thay đổi hoặc bị thu hồi quyền, thay đổi sẽ đồng bộ trên toàn bộ hệ thống. Tất cả các tài khoản truy cập cloud phải kích hoạt **xác thực đa yếu tố (MFA)** để giảm nguy cơ lộ mật khẩu[[52]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=One%20of%20the%20primary%20concerns,in%20transit%20and%20at%20rest). Bên cạnh đó, nguyên tắc **đặc quyền tối thiểu (least privilege)** phải được thực hiện nghiêm: mỗi tài khoản, mỗi dịch vụ chỉ được quyền cần thiết tối thiểu trên từng môi trường. Các quyền dư thừa (ví dụ một tài khoản dev mà có quyền admin trên cloud) cần được loại bỏ. Việc định kỳ **rà soát quyền (access review)** nên tiến hành hàng quý để phát hiện và sửa các thiết lập sai.
* **Mã hóa dữ liệu và bảo vệ luồng dữ liệu**: Dữ liệu nhạy cảm cần được mã hóa cả khi lưu trữ lẫn khi truyền trên mạng. Đối với dữ liệu tại chỗ, doanh nghiệp có thể dùng mã hóa ổ đĩa, cơ sở dữ liệu; trên cloud, hầu hết các dịch vụ đều cung cấp tùy chọn mã hóa (S3, Azure Storage encryption) – cần đảm bảo chúng được bật. Đặc biệt quan trọng là mã hóa các kết nối hybrid: thiết lập các đường VPN IPSec với thuật toán mã hóa mạnh cho đường truyền internet, hoặc dùng đường truyền riêng (Direct Connect/ExpressRoute) kết hợp với mã hóa lớp ứng dụng. Ngoài ra, có thể áp dụng giải pháp **CASB (Cloud Access Security Broker)** để giám sát và kiểm soát dữ liệu di chuyển lên cloud – CASB có thể phát hiện và ngăn chặn dữ liệu nhạy cảm (như số thẻ tín dụng, dữ liệu cá nhân) bị đưa lên cloud trái phép hoặc chia sẻ công khai. Về quản lý dữ liệu, cần phân loại rõ loại dữ liệu nào được phép đưa lên cloud, loại nào phải giữ on-prem để tuân thủ quy định, từ đó thiết lập chính sách kỹ thuật (ví dụ DLP – Data Loss Prevention) tương ứng.
* **Đánh giá cấu hình và tự động hóa bảo mật**: Một cách quan trọng để tránh misconfiguration là sử dụng các công cụ tự động **kiểm tra cấu hình bảo mật** trên cả hai môi trường. Các dịch vụ như AWS Config, Azure Security Center hoặc bên thứ ba (Prisma Cloud, Aqua Security) có thể quét tài khoản cloud để phát hiện cấu hình không an toàn (như cổng dịch vụ mở công khai, bucket không mã hóa). Tương tự, trong on-prem, các công cụ quản lý cấu hình tập trung (chef/puppet) có thể đảm bảo các máy chủ tuân thủ baseline bảo mật (cấu hình hệ điều hành, phần mềm). Khi triển khai hạ tầng bằng mã (IaC), có thể tích hợp bước kiểm tra bảo mật (security linting) trong pipeline để ngăn việc áp dụng cấu hình yếu lên môi trường thật. Ngoài ra, thực hiện **đánh giá bảo mật thường xuyên** (pentest, quét lỗ hổng) trên toàn bộ bề mặt hybrid (bao gồm ứng dụng, network on-prem và cloud) giúp tìm ra điểm yếu trước khi kẻ tấn công kịp khai thác. Việc này nên làm định kỳ và sau mỗi thay đổi lớn.
* **Giám sát và phản ứng (Monitoring & Incident Response)**: Xây dựng khả năng giám sát tập trung cho hybrid cloud. Doanh nghiệp cần thu thập nhật ký (log) từ cả hạ tầng on-prem (firewall, hệ thống IDS/IPS, server logs) lẫn cloud (CloudTrail/Azure Activity Log, VPC Flow Logs, v.v.) về một đầu mối (chẳng hạn hệ thống SIEM – Security Information and Event Management). Phân tích log bằng công cụ SIEM hoặc AI có thể giúp phát hiện những hành vi bất thường xuyên suốt hệ thống, ví dụ phát hiện nếu có đăng nhập từ địa chỉ IP lạ vào cả VPN nội bộ và tài khoản cloud cùng thời điểm (dấu hiệu tài khoản bị xâm nhập). Khi phát hiện sự cố, cần có sẵn **kế hoạch phản ứng (IR plan)** cho môi trường hybrid, bao gồm các bước cô lập phần bị ảnh hưởng (có thể phải tạm ngắt kết nối giữa on-prem và cloud để khoanh vùng), thông báo các bên liên quan và khôi phục. Các nhóm ứng cứu cần được đào tạo để hiểu kiến trúc hybrid và các công cụ trên cả hai môi trường. Một nghiên cứu chỉ ra tổ chức nào đầu tư vào an ninh mạng (con người, quy trình) sẽ có lợi ích lớn về lâu dài, thậm chí tăng cả doanh thu[[55]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=To%20effectively%20address%20these%20security,McKinsey%2C%202022) – nhấn mạnh việc an ninh không chỉ là chi phí mà còn là yếu tố thành công.
* **Bảo mật ứng dụng và API**: Với các API và ứng dụng phân tán, nên áp dụng tường lửa ứng dụng (WAF) và cổng API an toàn. WAF có thể chặn các cuộc tấn công web phổ biến (SQLi, XSS) trước khi chúng đi sâu vào hệ thống. Cổng API (API Gateway) nên có khả năng xác thực và giới hạn tốc độ (rate limiting) để ngăn lạm dụng API. Ngoài ra, cần triển khai các cơ chế **token hóa và ủy quyền** hiện đại (như OAuth 2.0, JWT) để các dịch vụ xác thực lẫn nhau an toàn, tránh dùng chung tài khoản tĩnh. Ở tầm vi mô, nếu dùng container, nên thực hiện quét lỗ hổng image container, áp dụng chính sách an ninh trong cụm Kubernetes (như Network Policy, kiểm soát Pod Security) để ngăn nguy cơ leo thang tấn công nếu một container bị xâm nhập.
* **Quản lý bản vá và cấu hình liên tục**: Môi trường hybrid dễ bị hở sườn nếu một bên cập nhật bản vá không kịp thời. Cần đồng bộ quy trình quản lý bản vá cho toàn bộ máy chủ, thiết bị mạng trên on-prem và cũng đảm bảo các dịch vụ cloud luôn áp dụng phiên bản mới nhất (cloud provider thường tự vá hạ tầng, nhưng phần do khách hàng quản lý như máy ảo, container thì phải tự lo). Công cụ quản lý bản vá tự động (WSUS, Patch Manager) có thể tích hợp cho cả hai môi trường. Đồng thời, xem xét sử dụng các dịch vụ bảo mật sẵn có từ nhà cung cấp cloud (như Amazon GuardDuty, Azure Defender) để giám sát mối đe dọa và gợi ý bản vá kịp thời.
* **Đào tạo nhân sự và quy trình**: Yếu tố con người vẫn luôn quan trọng. Cần đào tạo đội ngũ vận hành hiểu rõ các khác biệt và tích hợp khi làm việc với hybrid cloud. Họ phải nắm vững cấu hình an ninh cloud như cách thiết lập IAM, network security group, cũng như các kiến thức truyền thống (như bảo mật mạng LAN, firewall). Xây dựng văn hóa an ninh, trong đó mọi thay đổi kiến trúc hybrid đều phải xem xét khía cạnh bảo mật và tuân thủ. Thực hiện các buổi diễn tập định kỳ (ví dụ diễn tập ứng phó sự cố xâm nhập qua cloud) để các nhóm phối hợp nhuần nhuyễn.

Triển khai những giải pháp trên giúp tạo một **cách tiếp cận đa lớp (defense in depth)** cho hybrid cloud. Từ lớp mạng, lớp ứng dụng, cho đến quản trị con người đều phải có cơ chế bảo vệ. Khi có một lớp thất bại (ví dụ kẻ tấn công vượt qua VPN), lớp khác (như xác thực ứng dụng, phân quyền) sẽ ngăn chặn thiệt hại lan rộng. Sự phức tạp của hybrid cloud đòi hỏi một cái nhìn tổng thể: doanh nghiệp cần coi hybrid cloud như một thể thống nhất để áp dụng chiến lược bảo mật nhất quán, thay vì tư duy riêng lẻ từng silo on-prem hay cloud.

### 5.3. Tuân thủ các tiêu chuẩn và quy định

Bên cạnh bảo mật kỹ thuật, các doanh nghiệp triển khai hybrid cloud phải đặc biệt chú ý đến **tuân thủ (compliance)** – tức đáp ứng các yêu cầu luật pháp, tiêu chuẩn trong lĩnh vực hoạt động. Việc tuân thủ trong bối cảnh hybrid cloud có thể phức tạp hơn do dữ liệu và quy trình trải rộng qua nhiều hạ tầng và có sự tham gia của bên thứ ba (nhà cung cấp cloud). Dưới đây là những khía cạnh chính về tuân thủ và cách thức đảm bảo:

* **Tuân thủ quy định về bảo vệ dữ liệu cá nhân**: Nhiều quốc gia và khu vực có luật nghiêm ngặt về bảo vệ dữ liệu cá nhân, như **GDPR** của EU, **CCPA** của California, **PDPA** của Singapore, v.v. Các luật này thường quy định việc thu thập, lưu trữ, xử lý dữ liệu cá nhân phải đảm bảo quyền riêng tư, bảo mật, và đặc biệt là **giới hạn chuyển dữ liệu ra nước ngoài**. Triển khai hybrid cloud, doanh nghiệp phải nắm rõ dữ liệu cá nhân (ví dụ thông tin khách hàng) đang nằm ở đâu. Nếu dùng cloud đặt máy chủ ngoài lãnh thổ, cần đánh giá có vi phạm quy tắc chuyển dữ liệu không. Một số trường hợp, doanh nghiệp chọn kiến trúc hybrid để đáp ứng yêu cầu này: dữ liệu cá nhân được lưu và xử lý trong private cloud nội địa, còn các workload khác ít nhạy cảm hơn mới chạy trên public cloud toàn cầu. Ngoài ra, khi dùng dịch vụ cloud, cần ký **thỏa thuận xử lý dữ liệu (DPA)** với nhà cung cấp, trong đó họ cam kết tuân thủ các điều khoản như GDPR, hỗ trợ doanh nghiệp đáp ứng yêu cầu (ví dụ cung cấp công cụ xóa dữ liệu người dùng khi có yêu cầu theo GDPR). Tóm lại, tuân thủ bảo vệ dữ liệu đòi hỏi **quản trị vòng đời dữ liệu chặt chẽ** và minh bạch trong hybrid cloud.
* **Chứng chỉ và tiêu chuẩn bảo mật**: Doanh nghiệp trong các ngành như tài chính, y tế, dịch vụ công thường phải tuân theo các tiêu chuẩn bảo mật CNTT như **ISO/IEC 27001** (tiêu chuẩn quốc tế về hệ thống quản lý an toàn thông tin), **PCI-DSS** (tiêu chuẩn bảo mật dữ liệu thẻ thanh toán), **HIPAA** (Đạo luật về di động và trách nhiệm bảo hiểm y tế của Mỹ, yêu cầu bảo mật thông tin y tế cá nhân), hoặc tiêu chuẩn của ngành (ví dụ chuẩn **MAS** cho ngân hàng ở Singapore). Khi đưa hệ thống lên hybrid cloud, doanh nghiệp cần đảm bảo các thành phần trên cloud cũng đáp ứng các tiêu chuẩn này tương đương hệ thống nội bộ. Tin tốt là hầu hết các nhà cung cấp lớn (AWS, Azure, Google) đều đã đạt chứng chỉ như ISO 27001, PCI-DSS, HIPAA... cho hạ tầng của họ[[56]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=access%20controls%2C%20and%20regular%20security,data%20and%20maintains%20customer%20trust). Điều đó nghĩa là nếu cấu hình đúng, doanh nghiệp **có thể** vận hành hệ thống tuân thủ trên cloud. Tuy nhiên, tránh hiểu lầm: **trách nhiệm tuân thủ chia sẻ** – nhà cung cấp cloud đảm bảo nền tảng họ tuân thủ, còn doanh nghiệp vẫn phải đảm bảo phần cấu hình và sử dụng dịch vụ của mình tuân thủ. Ví dụ, AWS có chứng chỉ PCI-DSS cho dịch vụ, nhưng nếu doanh nghiệp lưu số thẻ tín dụng ở dạng không mã hóa trên S3 rồi vô tình mở public, thì vẫn vi phạm PCI-DSS. Do vậy, cần nghiên cứu kĩ các hướng dẫn tuân thủ cho cloud (các provider thường cung cấp whitepaper về PCI, HIPAA on AWS/Azure) để cấu hình phù hợp.
* **Địa điểm đặt dữ liệu và hệ thống (Data Sovereignty)**: Một số quốc gia yêu cầu hệ thống CNTT phục vụ cho công dân nước họ phải được triển khai trong nước. Ví dụ, chính phủ Việt Nam yêu cầu dữ liệu cá nhân quan trọng phải lưu trữ tại Việt Nam, Trung Quốc có luật an ninh mạng quy định dữ liệu của người TQ phải ở trong TQ, v.v. Điều này ảnh hưởng đến kiến trúc hybrid: doanh nghiệp có thể phải thiết lập private cloud hoặc dùng region cloud đặt tại quốc gia sở tại để phục vụ người dùng địa phương, thay vì truy cập qua region nước ngoài. Các hãng cloud lớn hiện đều có nhiều **khu vực (region)** trên thế giới, cho phép doanh nghiệp lựa chọn nơi đặt dữ liệu để tuân thủ quy định. Hybrid cloud tạo điều kiện cho việc này: công ty có thể giữ hạ tầng on-premise tại những nước yêu cầu chủ quyền dữ liệu, trong khi vẫn kết nối với đám mây toàn cầu cho các phần việc khác. Tuy nhiên, cần đánh giá kỹ luồng dữ liệu để chắc chắn không có dữ liệu nhạy cảm nào âm thầm chảy sang vùng cấm. Ví dụ, tắt các tính năng gửi log, diagnostic từ hệ thống nội địa sang server cloud ở Mỹ nếu luật không cho phép.
* **Quản lý rủi ro bên thứ ba**: Khi dùng cloud tức là doanh nghiệp đang *outsourcing* một phần hạ tầng cho bên thứ ba. Nhiều chuẩn và quy định (như ISO 27001, hay quy định ngành ngân hàng) đòi hỏi đánh giá rủi ro nhà cung cấp và có biện pháp giám sát. Trong bối cảnh hybrid cloud, doanh nghiệp cần làm việc với nhà cung cấp cloud để hiểu rõ trách nhiệm của mỗi bên (thường được mô tả trong tài liệu *Shared Responsibility Model* của provider). Cũng nên xem xét các **báo cáo kiểm toán độc lập** của nhà cung cấp (ví dụ báo cáo SOC 2 Type II) để có niềm tin họ vận hành đúng quy trình bảo mật. Một số ngành còn yêu cầu thông báo cho cơ quan quản lý khi sử dụng dịch vụ cloud (ví dụ ngân hàng châu Âu phải tuân theo hướng dẫn của EBA – European Banking Authority – khi đưa dịch vụ ra cloud[[57]](https://www.eba.europa.eu/documents/10180/2422294/85702de4-e7a3-4c92-be75-4d8903dabf89/Session%202%20-%20HSBC%20Cloud%20-%2017%20Oct%202018.pdf#:~:text=,AWS)). Do đó, bộ phận tuân thủ cần được tham gia ngay từ giai đoạn thiết kế kiến trúc hybrid để đảm bảo đáp ứng các thủ tục pháp lý.
* **Công cụ và chứng từ hỗ trợ tuân thủ**: Để dễ dàng hơn trong quản lý tuân thủ, doanh nghiệp có thể tận dụng các công cụ do nhà cung cấp cloud cung cấp. Chẳng hạn, Azure có **Compliance Manager** giúp đánh giá mức độ tuân thủ của hệ thống so với các tiêu chuẩn (GDPR, ISO, v.v.), AWS có các **Artifact** để tải xuống chứng chỉ, báo cáo kiểm toán của AWS. Việc chuẩn bị sẵn các tài liệu, bằng chứng này sẽ hữu ích khi có đợt kiểm toán hoặc thanh tra. Bên cạnh đó, cần cập nhật chính sách nội bộ về bảo mật, tuân thủ để bao hàm luôn môi trường cloud. Ví dụ, chính sách phân loại dữ liệu nên cập nhật rằng dữ liệu loại A (nhạy cảm cao) không được đưa lên public cloud trừ khi mã hóa và phê duyệt đặc biệt, v.v.
* **Kiểm toán và đánh giá định kỳ**: Cuối cùng, cần lên lịch kiểm toán nội bộ hoặc thuê kiểm toán độc lập định kỳ để đánh giá hệ thống hybrid có tuân thủ đúng các yêu cầu không. Việc này bao gồm review cấu hình, log, quy trình. Kiểm toán nên bao trùm cả on-prem và cloud. Kết quả kiểm toán sẽ chỉ ra điểm nào chưa đáp ứng (ví dụ phát hiện server cloud chưa bật log đầy đủ theo yêu cầu ISO 27001) để khắc phục kịp thời. Thực hành này giúp doanh nghiệp luôn sẵn sàng cho các đợt đánh giá chính thức từ bên ngoài và tránh bị phạt hoặc sự cố do vi phạm tuân thủ.

Tóm lại, **tuân thủ trong hybrid cloud là sự tiếp nối của các yêu cầu truyền thống vào một môi trường mới**, đòi hỏi doanh nghiệp điều chỉnh kiến trúc, quy trình cho phù hợp. May mắn là các nhà cung cấp cloud lớn đều nhận thức rõ điều này và cung cấp nhiều công cụ hỗ trợ tuân thủ[[56]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=access%20controls%2C%20and%20regular%20security,data%20and%20maintains%20customer%20trust). Doanh nghiệp cần chủ động sử dụng các công cụ đó và tích hợp chúng vào hệ thống quản lý tuân thủ nội bộ. Bằng cách cẩn trọng trong quản lý dữ liệu, chọn nơi lưu trữ, thiết lập cấu hình và quy trình đúng chuẩn, hybrid cloud có thể được triển khai mà vẫn đáp ứng các đòi hỏi khắt khe của ngành và luật pháp.

## 6. Kết luận và hướng phát triển

Hybrid cloud đã chứng tỏ là một mô hình quan trọng trong lộ trình phát triển hạ tầng CNTT hiện đại. Thông qua các phần trình bày, có thể thấy **điện toán đám mây lai** mang lại cho doanh nghiệp khả năng kết hợp tốt nhất của hai thế giới: **sự linh hoạt, quy mô** của đám mây công cộng và **sự kiểm soát, bảo mật** của đám mây riêng. Mô hình này ra đời để giải quyết những hạn chế của cách tiếp cận "thuần công cộng" hay "thuần nội bộ", và thực tế triển khai tại nhiều tổ chức lớn đã khẳng định giá trị của nó trong việc hỗ trợ chuyển đổi số một cách an toàn, tuân thủ.

Trong phần mở đầu, luận văn đã nêu bối cảnh và lý do ra đời của hybrid cloud – đó là nhu cầu cấp thiết của doanh nghiệp khi vừa muốn tận dụng tài nguyên on-demand, vừa phải đáp ứng các ràng buộc về bảo mật, tuân thủ. Phần cơ sở lý thuyết cung cấp cái nhìn rõ nét về khái niệm hybrid cloud, đặc điểm và so sánh với các mô hình khác. **Hybrid cloud không thay thế hoàn toàn public hay private cloud, mà đóng vai trò bổ trợ, cầu nối**, giúp nhiều tổ chức lần đầu bước chân lên mây một cách từng bước, giảm thiểu rủi ro[[10]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=effective%20than%20private%20ones,allows%20users%20to%20migrate%20gradually). Kiến trúc kỹ thuật của hybrid cloud khá phức tạp, đòi hỏi nhiều thành phần và công nghệ, từ kết nối mạng, nền tảng container cho đến lớp quản lý hợp nhất. Chính nhờ sự trưởng thành của những công nghệ này (như Kubernetes, VPN, SD-WAN...) mà hybrid cloud mới thực sự khả thi và hiệu quả ở quy mô lớn như hiện nay.

Các ví dụ ứng dụng thực tế trong doanh nghiệp đã minh họa sinh động cách hybrid cloud được vận dụng: từ việc xử lý mùa cao điểm thương mại điện tử, triển khai dịch vụ tài chính đám mây riêng cho đến tối ưu chuỗi cung ứng toàn cầu. Bất kể ngành nghề, một chiến lược hybrid tốt có thể đem lại **lợi thế cạnh tranh** – tốc độ ra mắt dịch vụ nhanh hơn, trải nghiệm khách hàng tốt hơn, và chi phí vận hành tối ưu hơn[[58]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Despite%20these%20challenges%2C%20many%20enterprises,for%20their%20hybrid%20cloud%20infrastructure)[[33]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20adoption%20rate%20of%20hybrid,effectiveness%20in%20enterprise%20IT%20environments). Tuy nhiên, hybrid cloud không phải không có thách thức: đặc biệt về bảo mật và quản lý, do tính phức tạp của hệ thống tăng lên đáng kể. Phần bảo mật và tuân thủ đã phân tích sâu những rủi ro cũng như đề xuất các biện pháp để khắc phục. Đây là lời nhắc rằng doanh nghiệp phải đầu tư tương xứng vào năng lực an ninh mạng và quản trị rủi ro khi triển khai hybrid cloud – không thể chủ quan vì chỉ một lỗ hổng nhỏ cũng có thể ảnh hưởng cả hệ thống liên kết.

Nhìn về **hướng phát triển**, hybrid cloud được dự đoán sẽ tiếp tục là mô hình chủ đạo trong những năm tới, ít nhất là trung hạn. Theo khảo sát của Forrester, 73% doanh nghiệp đang lên kế hoạch duy trì hoặc mở rộng hybrid cloud trong vòng hai năm tới[[59]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Hybrid%20cloud%20computing%20allows%20enterprises,agility%2C%20innovation%2C%20and%20cost%20savings). Một số xu hướng định hình tương lai hybrid cloud gồm:

* **Sự hội tụ với điện toán biên (Edge Computing)**: Ngày càng nhiều thiết bị IoT và nhu cầu xử lý gần nguồn dữ liệu để giảm độ trễ. Hybrid cloud sẽ mở rộng để tích hợp chặt chẽ với các **edge cloud**. Các nhà cung cấp giới thiệu kiến trúc *distributed cloud*, trong đó đám mây công cộng có thể “trải dài” đến biên thông qua các thiết bị/đám mây mini đặt tại chỗ khách hàng. Ví dụ, AWS Outposts hoặc Azure Stack Edge chính là những cầu nối như vậy, cho phép chạy dịch vụ cloud ngay tại môi trường on-prem nhưng quản lý đồng nhất từ cloud. Điều này làm mờ ranh giới giữa private-public hơn nữa, hướng tới tương lai **đa môi trường liền mạch**. Dự báo có tới 70% tổ chức sẽ triển khai giải pháp edge trong vài năm tới, và hybrid cloud sẽ là bộ khung kết nối edge với cloud trung tâm[[60]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Another%20key%20trend%20in%20hybrid,time).
* **Multi-cloud trở thành tiêu chuẩn**: Không chỉ dừng ở hai môi trường, nhiều doanh nghiệp sẽ sử dụng 2-3 nền tảng đám mây công cộng kết hợp (multi-cloud) bên cạnh hạ tầng riêng, tạo nên kiến trúc phức hợp hơn nữa. Điều này thúc đẩy nhu cầu về các **công cụ quản lý đa đám mây** thống nhất, các lớp trừu tượng đa cloud để nhà phát triển không phải lo lắng về sự khác biệt nền tảng. Các công cụ open-source như Kubernetes, Terraform sẽ ngày càng phổ biến như một “ngôn ngữ chung” để làm việc với multi/hybrid cloud. Thêm vào đó, các tiêu chuẩn mở về tương tác đám mây (như Open Cloud Computing Interface, Open Service Broker) có thể phát triển, được hỗ trợ bởi tổ chức chuẩn hóa, giúp tăng tính **liên vận hành (interoperability)** giữa các cloud. Mục tiêu là giảm thiểu *vendor lock-in*, cho phép workload di chuyển tự do hơn tùy theo nhu cầu, tương tự cách ngành container đã làm được.
* **Tập trung vào tối ưu chi phí và hiệu năng**: Khi hạ tầng hybrid phình to, tối ưu hóa sẽ là mối quan tâm lớn. Sẽ có nhiều giải pháp quản trị thông minh xuất hiện: chẳng hạn **AI Ops** – dùng trí tuệ nhân tạo để tự động đề xuất điều chuyển workload giữa on-prem và cloud nhằm tối ưu chi phí hoặc hiệu năng theo thời điểm (ví dụ giờ cao điểm chạy on-prem để tiết kiệm băng thông cloud, giờ thấp điểm đẩy lên cloud để tắt bớt server nội bộ tiết kiệm điện). Các công cụ dự báo chi phí đa đám mây giúp tài chính dự trù tốt hơn. Đồng thời, các dịch vụ mới như **serverless** và **Function-as-a-Service** sẽ được tận dụng trong hybrid cloud để tăng hiệu quả – code có thể chạy trên bất kỳ hạ tầng nào mà không cần quản lý server, đem lại khả năng mở rộng linh hoạt hơn nữa. Theo báo cáo, 75% doanh nghiệp đã và đang định dùng serverless trong hệ thống của họ[[61]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20future%20of%20hybrid%20cloud,can%20enhance%20security%20and%20transparency); tích hợp serverless giữa on-prem (qua nền tảng như OpenFaaS) và public cloud có thể là bước tiến kế tiếp.
* **Nâng cao an ninh bằng cách tận dụng công nghệ mới**: Lĩnh vực bảo mật hybrid cloud sẽ tiếp tục sôi động. Các kỹ thuật như **bảo mật dựa trên phần cứng** (Hardware enclaves, ví dụ AWS Nitro Enclaves) cho phép bảo vệ dữ liệu nhạy cảm ngay cả khi đưa lên cloud, hoặc **mã hóa đồng homomorphic** cho phép xử lý dữ liệu mà không cần giải mã, sẽ dần khả thi và có thể được ứng dụng để giải quyết mối lo ngại về tin cậy cloud. Ngoài ra, các sáng kiến về **Zero Trust Cloud** được thúc đẩy, trong đó mỗi thành phần, mỗi kết nối trong hybrid cloud đều phải xác thực, mã hóa – biến cloud thành phần mở rộng thực sự an toàn của mạng doanh nghiệp. Song song, chúng ta có thể thấy nhiều quy định mới ra đời để quản lý việc sử dụng cloud (ví dụ luật về bảo vệ dữ liệu ngày càng lan rộng), nên sự tuân thủ sẽ càng được chú trọng. Doanh nghiệp hybrid cloud tương lai có thể phải tuân theo những framework như **GAIA-X** (sáng kiến cloud châu Âu) hoặc chứng minh tuân thủ liên tục qua các báo cáo tự động từ hệ thống.
* **Ảnh hưởng của các công nghệ mới nổi**: Công nghệ như **blockchain** cũng có thể đóng vai trò hỗ trợ hybrid cloud, chẳng hạn dùng blockchain để tạo kênh audit tin cậy ghi lại các hoạt động cross-cloud, tăng tính minh bạch và bất biến (một số dự án đã nghiên cứu blockchain cho quản lý cấu hình multi-cloud). Ngoài ra, **máy tính lượng tử** tuy còn sớm, nhưng trong tương lai nếu trở thành dịch vụ cloud (Quantum Computing as a Service), doanh nghiệp rất có thể sử dụng nó như phần mở rộng trong hybrid cloud để chạy những tác vụ đặc thù siêu nhanh, sau đó trả kết quả về hệ thống chính. Tất cả đều hướng đến viễn cảnh một môi trường điện toán hợp nhất, linh hoạt chưa từng có.

Tổng kết lại, hybrid cloud đã, đang và sẽ tiếp tục là một yếu tố chủ chốt trong chiến lược CNTT của nhiều tổ chức. Nó không phải viên đạn bạc cho mọi vấn đề, nhưng nếu được thiết kế và quản trị đúng đắn, hybrid cloud mang lại **sự cân bằng tối ưu** giữa đổi mới và ổn định – điều mà mọi doanh nghiệp đều khao khát trong kỷ nguyên số. Trong chặng đường phía trước, với sự hỗ trợ của các công nghệ và phương pháp mới, hybrid cloud hứa hẹn còn phát triển mạnh mẽ hơn, trở thành **mô hình đám mây hợp nhất (unified cloud model)**, nơi ranh giới giữa các môi trường ngày càng mờ đi, cho phép CNTT phục vụ kinh doanh một cách linh hoạt, an toàn chưa từng có.

**Tài liệu tham khảo chọn lọc:**

【2】Mell, P., & Grance, T. (2011). *NIST SP 800-145: The NIST Definition of Cloud Computing*[[5]](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf#:~:text=Hybrid%20cloud,libraries%2C%20services%2C%20and%20tools%20from). National Institute of Standards and Technology.

【3】Haff, G. (2017). *The changing face of the hybrid cloud*[[3]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=NIST%27s%20original%20hybrid%20cloud%20definition,capacity%20wherever%20it%20was%20cheapest)[[7]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=The%20widespread%20adoption%20of%20containers,testing%2C%20and%20finally%20to%20production). Opensource.com (Red Hat).

【6】Quantum News. (2024). *Innovations in hybrid cloud technologies for enterprise applications*[[62]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=the%20cost,premises%20deployments%20%28Gartner%2C%202020)[[63]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=One%20of%20the%20primary%20concerns,in%20transit%20and%20at%20rest). QuantumZeitgeist.com.

【21】Hougen, A. (2025). *Cloud Deployment Models: Definition & Types*[[11]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Factors%3APublic%20Cloud%20Private%20Cloud%20Hybrid,portion%20shared%20with%20other%20clients)[[12]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Setup%20Complexity%20Easy%20Complex%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies). Cloudwards.net.

【23】Red Hat. (2023). *Hybrid cloud architecture – What is hybrid cloud?*[[2]](https://developers.redhat.com/topics/hybrid-cloud-architecture#:~:text=Hybrid%20cloud%20setups%20have%20become,sensitivity%20and%20high%20volume%20requirements). Redhat.com.

【9】Quantum News. (2024). *Case Studies Of Successful Enterprise Deployments*[[50]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=According%20to%20a%20study%20by,IDG%2C%202022)[[51]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20adoption%20of%20hybrid%20cloud,sized%20businesses). QuantumZeitgeist.com.

【17】Haynes, I. (2022). *HSBC’s Cloud Strategy*[[29]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=The%20power%20of%20Cloud%20enables,vendor%20strengths%20and%20geographical%20coverage)[[64]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=industry%20leading%20technology%20from%20Google%2C,vendor%20strengths%20and%20geographical%20coverage). CIOReview Europe (aws.ciorevieweurope.com).

【8】Quantum News. (2024). *Public Cloud Service Provider Selection Criteria*[[65]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Security%20is%20a%20top%20priority,data%20and%20maintains%20customer%20trust)[[56]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=access%20controls%2C%20and%20regular%20security,data%20and%20maintains%20customer%20trust). QuantumZeitgeist.com.

【38】Amazon Web Services. (2016). *Netflix Case Study - AWS*[[66]](https://aws.amazon.com/solutions/case-studies/netflix-case-study/#:~:text=Online%20content%20provider%20Netflix%20can,mobile%20devices%20such%20as%20iPhones)[[67]](https://aws.amazon.com/solutions/case-studies/netflix-case-study/#:~:text=Netflix%2C%20one%20of%20the%20world%E2%80%99s,performance%20of%20its%20global%20service). AWS Case Study Collection.

[[1]](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf#:~:text=Cloud%20computing%20is%20a%20model,models%2C%20and%20four%20deployment%20models) [[4]](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf#:~:text=Hybrid%20cloud,for%20load%20balancing%20between%20clouds) [[5]](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf#:~:text=Hybrid%20cloud,libraries%2C%20services%2C%20and%20tools%20from) NIST SP 800-145, The NIST Definition of Cloud Computing

<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>

[[2]](https://developers.redhat.com/topics/hybrid-cloud-architecture#:~:text=Hybrid%20cloud%20setups%20have%20become,sensitivity%20and%20high%20volume%20requirements) [[26]](https://developers.redhat.com/topics/hybrid-cloud-architecture#:~:text=Hybrid%20cloud%20systems%20also%20enable,for%20a%20fully%20private%20solution) Hybrid cloud architecture | Red Hat Developer

<https://developers.redhat.com/topics/hybrid-cloud-architecture>

[[3]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=NIST%27s%20original%20hybrid%20cloud%20definition,capacity%20wherever%20it%20was%20cheapest) [[7]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=The%20widespread%20adoption%20of%20containers,testing%2C%20and%20finally%20to%20production) [[8]](https://opensource.com/article/17/7/hybrid-cloud#:~:text=Specifications%20developed%20under%20the%20auspices,stable%20runtime%20and%20image%20specs) ﻿The changing face of the hybrid cloud | Opensource.com

<https://opensource.com/article/17/7/hybrid-cloud>

[[6]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=A%20hybrid%20cloud%20model%20allows,as%20PaaS%20and%20IaaS%20services) [[20]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=On) [[21]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=However%2C%20on,premises%20infrastructure) [[22]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=Wide%20Area%20Networks%20,secure%20connection%20between%20two%20networks) [[23]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=APIs%20are%20employed%20to%20facilitate,secure%20connection%20between%20two%20networks) [[25]](https://www.hava.io/blog/hybrid-cloud-diagramming#:~:text=,transformation%2C%20disaster%20recovery%20and%20development%2Ftesting) Hybrid Cloud Diagrams

<https://www.hava.io/blog/hybrid-cloud-diagramming>

[[9]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=defined%20by%20NIST.%20,allows%20users%20to%20migrate%20gradually) [[10]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=effective%20than%20private%20ones,allows%20users%20to%20migrate%20gradually) [[11]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Factors%3APublic%20Cloud%20Private%20Cloud%20Hybrid,portion%20shared%20with%20other%20clients) [[12]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Setup%20Complexity%20Easy%20Complex%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies) [[13]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Access%20Type%20No%20direct%20access,Complex%20Moderate%20Very%20complex%20Moderate) [[14]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=or%20organizations%20All%20companies%20or,to%20maintain%20Lower%20due%20to) [[15]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Cost%20Efficiency%20High%20Low%20Moderate,corporations%20%26%20multinational%20enterprises%20Companies) [[16]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Scalability%20High%20Low%20High%20Low,to%20maintain%20Lower%20due%20to) [[17]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Reliability%20Low%20High%20Moderate%20High,corporations%20%26%20multinational%20enterprises%20Companies) [[18]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Public%20clouds%20are%20the%20best,be%20the%20way%20to%20go) [[19]](https://www.cloudwards.net/cloud-deployment-models/#:~:text=Best%20Fit%20Most%20companies%20Large,with%20very%20specific%20platform%20requirements) What Are the 5 Cloud Deployment Models [Explained & Compared]

<https://www.cloudwards.net/cloud-deployment-models/>

[[24]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=To%20mitigate%20these%20risks%2C%20enterprises,Cloud%20Security%20Alliance%2C%202019) [[27]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20benefits%20of%20hybrid%20cloud,based%20infrastructure) [[28]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Hybrid%20cloud%20computing%20has%20become,risk%20management%2C%20and%20data%20analytics) [[30]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Another%20significant%20risk%20is%20the,regularly%20updated%20to%20prevent%20vulnerabilities) [[31]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=However%2C%20implementing%20hybrid%20clouds%20also,of%20security%20and%20compliance%20standards) [[33]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20adoption%20rate%20of%20hybrid,effectiveness%20in%20enterprise%20IT%20environments) [[34]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=effectiveness%20in%20enterprise%20IT%20environments) [[46]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=One%20notable%20example%20of%20successful,customer%20experience%2C%20and%20reduce%20costs) [[47]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=architecture%20that%20combines%20on,customer%20experience%2C%20and%20reduce%20costs) [[48]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20use%20of%20hybrid%20cloud,customer%20experience%2C%20and%20reduce%20costs) [[49]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Another%20example%20is%20the%20use,customer%20experience%2C%20and%20reduce%20costs) [[50]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=According%20to%20a%20study%20by,IDG%2C%202022) [[51]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20adoption%20of%20hybrid%20cloud,sized%20businesses) [[52]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=One%20of%20the%20primary%20concerns,in%20transit%20and%20at%20rest) [[53]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=In%20addition%20to%20these%20risks%2C,demands%20of%20hybrid%20cloud%20environments) [[54]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20hybrid%20cloud%20market%20is,in%20%2844) [[55]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=To%20effectively%20address%20these%20security,McKinsey%2C%202022) [[56]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=access%20controls%2C%20and%20regular%20security,data%20and%20maintains%20customer%20trust) [[58]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Despite%20these%20challenges%2C%20many%20enterprises,for%20their%20hybrid%20cloud%20infrastructure) [[59]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Hybrid%20cloud%20computing%20allows%20enterprises,agility%2C%20innovation%2C%20and%20cost%20savings) [[60]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Another%20key%20trend%20in%20hybrid,time) [[61]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=The%20future%20of%20hybrid%20cloud,can%20enhance%20security%20and%20transparency) [[62]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=the%20cost,premises%20deployments%20%28Gartner%2C%202020) [[63]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=One%20of%20the%20primary%20concerns,in%20transit%20and%20at%20rest) [[65]](https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/#:~:text=Security%20is%20a%20top%20priority,data%20and%20maintains%20customer%20trust) Innovations In Hybrid Cloud Technologies For Enterprise Applications

<https://quantumzeitgeist.com/innovations-in-hybrid-cloud-technologies-for-enterprise-applications/>

[[29]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=The%20power%20of%20Cloud%20enables,vendor%20strengths%20and%20geographical%20coverage) [[41]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=industry%20leading%20technology%20from%20Google%2C,vendor%20strengths%20and%20geographical%20coverage) [[42]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=means%20that%20we%20can%20create,flow%20forecasting%20and%20business%20insights) [[43]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=Ultimately%20our%20use%20of%20Cloud,Users%20benefit%20from%20account) [[44]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=Cloud%20efficiency%20is%20particularly%20important,chain%20by%202030%20or%20sooner) [[45]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=Our%20Cloud%20providers%20share%20our,Cloud%20we%20use%20zero%20energy) [[64]](https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html#:~:text=industry%20leading%20technology%20from%20Google%2C,vendor%20strengths%20and%20geographical%20coverage) HSBC'S Cloud Strategy

<https://aws.ciorevieweurope.com/cxoinsight/hsbc-s-cloud-strategy-nwid-1234.html>

[[32]](https://cloud.google.com/customers/featured/hsbc#:~:text=HSBC%20Customer%20Hub%20,automation%20built%20in%20along) HSBC Customer Hub | Google Cloud

<https://cloud.google.com/customers/featured/hsbc>

[[35]](https://aws.amazon.com/solutions/case-studies/netflix-case-study/#:~:text=Online%20content%20provider%20Netflix%20can,mobile%20devices%20such%20as%20iPhones) [[36]](https://aws.amazon.com/solutions/case-studies/netflix-case-study/#:~:text=Netflix%20Delivers%20Billions%20of%20Hours,Globally%20by%20Running%20on%20AWS) [[66]](https://aws.amazon.com/solutions/case-studies/netflix-case-study/#:~:text=Online%20content%20provider%20Netflix%20can,mobile%20devices%20such%20as%20iPhones) [[67]](https://aws.amazon.com/solutions/case-studies/netflix-case-study/#:~:text=Netflix%2C%20one%20of%20the%20world%E2%80%99s,performance%20of%20its%20global%20service) Netflix Case Study

<https://aws.amazon.com/solutions/case-studies/netflix-case-study/>

[[37]](https://nordcloud.com/case-studies/bmw-group/#:~:text=The%20client) [[38]](https://nordcloud.com/case-studies/bmw-group/#:~:text=The%20BMW%20Group%20wanted%20a,both%20Microsoft%20Azure%20and%20AWS) [[39]](https://nordcloud.com/case-studies/bmw-group/#:~:text=%2A%2050,and%20management%20of%20cloud%20resources) [[40]](https://nordcloud.com/case-studies/bmw-group/#:~:text=Multi) BMW Group - Case study - Nordcloud

<https://nordcloud.com/case-studies/bmw-group/>

[[57]](https://www.eba.europa.eu/documents/10180/2422294/85702de4-e7a3-4c92-be75-4d8903dabf89/Session%202%20-%20HSBC%20Cloud%20-%2017%20Oct%202018.pdf#:~:text=,AWS) [PDF] Cloud Computing

<https://www.eba.europa.eu/documents/10180/2422294/85702de4-e7a3-4c92-be75-4d8903dabf89/Session%202%20-%20HSBC%20Cloud%20-%2017%20Oct%202018.pdf>