



10 XU HƯỚNG CÔNG NGHỆ CHIẾN LƯỢC VÀ TẦM NHÌN QUẢN TRỊ TƯƠNG LAI

“

Trong bối cảnh thế giới đã bước sang ngưỡng cửa của năm 2026, dòng chảy đổi mới sáng tạo không còn diễn ra theo những bước tiến tuần tự mà chuyển sang trạng thái bùng nổ theo cấp số nhân. Sự hội tụ giữa trí tuệ nhân tạo (AI), các hệ thống tự chủ vật lý và các rủi ro địa chính trị đang buộc các tổ chức phải tái định nghĩa lại toàn bộ cấu trúc vận hành của mình. Nếu như giai đoạn trước đây được đánh dấu bằng sự say mê thử nghiệm với các mô hình ngôn ngữ lớn sơ khai, thì giai đoạn từ năm 2026 trở đi sẽ chứng kiến sự chuyển dịch mang tính quyết định từ thử nghiệm sang tác động thực tế. Các nhà lãnh đạo công nghệ hiện nay không còn coi đổi mới là một dự án phụ mà phải tích hợp nó vào lõi chiến lược để đảm bảo khả năng phục hồi và tăng trưởng bền vững.

”





10 xu hướng công nghệ chiến lược

Dưới đây là phân tích chuyên sâu về 10 xu hướng công nghệ chiến lược sẽ định hình lại tương lai kinh doanh và đời sống xã hội trong những năm tới.

1. Nền tảng phát triển thuần AI: Tái cấu trúc quy trình kỹ thuật phần mềm thông qua AI tạo sinh

Các nền tảng phát triển thuần AI sử dụng AI tạo sinh để tăng tốc quá trình tạo phần mềm, cho phép các nhóm nhỏ, linh hoạt hoặc thậm chí là các chuyên gia nghiệp vụ xây dựng ứng dụng nhanh hơn với khả năng quản trị tích hợp. Xu hướng này không chỉ dừng lại ở việc hỗ trợ viết mã mà còn tiến tới và sử dụng các tác nhân AI để cùng sáng tạo ứng dụng. Gartner dự báo rằng, đến năm 2030, khoảng 80% các tổ chức sẽ chuyển đổi các đội ngũ phần mềm lớn hiện tại thành các nhóm nhỏ hơn, được tăng cường năng lực bởi AI. Điều này buộc các giám đốc thông tin (CIO) phải tư duy lại toàn bộ cách thức kỹ sư hóa phần mềm, chuyển dịch từ mô hình “xây dựng hay mua” sang tự đổi mới tại chỗ với năng suất cực cao.

2. Nền tảng siêu máy tính AI: Xây dựng hạ tầng chuyên biệt cho kỷ nguyên mô hình ngôn ngữ khổng lồ

Sự phức tạp ngày càng tăng của AI đòi hỏi một loại hạ tầng mục đích đặc biệt, kết hợp giữa CPU, GPU, các chip chuyên dụng (AI ASICs) và máy tính lấy cảm hứng từ não bộ (neuromorphic computing). Những hệ thống này cung cấp hiệu suất và khả năng mở rộng chưa từng có để điều phối các khối lượng công việc phức tạp trong học máy, phân tích dữ liệu và mô phỏng. Đến năm 2028, dự kiến hơn 40% các doanh nghiệp hàng đầu sẽ áp dụng các mô hình máy tính lai vào các quy trình làm việc quan trọng, tăng đáng kể so với mức 8% hiện nay. Việc đầu tư vào siêu máy tính không chỉ giúp tăng tốc đổi mới mà còn giúp các doanh nghiệp tối ưu hóa chi phí năng lượng và khả năng xử lý các mô hình AI có quy mô siêu lớn.

3. Điện toán bảo mật: Lá chắn bảo vệ dữ liệu trong quá trình xử lý tại môi trường lai và ít tin cậy

Điện toán bảo mật bảo vệ dữ liệu ngay trong quá trình sử dụng bằng cách cách ly các khối lượng công

việc bên trong môi trường thực thi tin cậy (TEEs) dựa trên phần cứng. Điều này cho phép các tổ chức xử lý dữ liệu nhạy cảm một cách an toàn ngay cả trên các hạ tầng chung hoặc hạ tầng từ các nhà cung cấp dịch vụ đám mây. Dự kiến đến năm 2029, hơn 75% các hoạt động xử lý dữ liệu trên các hạ tầng sẽ được bảo mật bằng công nghệ này. Đây là yếu tố sống còn cho các ngành chịu sự quản lý chặt chẽ như y tế, tài chính, đồng thời hỗ trợ các kiến trúc đa đám mây và đa khu vực pháp lý theo mô hình zero trust (zero trust là mô hình luôn luôn xác thực, không bao giờ mặc định tin tưởng).

4. Hệ thống đa tác nhân: Sự chuyển dịch từ công cụ hỗ trợ đơn lẻ sang mạng lưới cộng tác tự chủ

Các hệ thống đa tác nhân bao gồm mạng lưới các tác nhân AI chuyên biệt cộng tác với nhau để thực hiện các mục tiêu chung và giải quyết các quy trình phức tạp nhiều bước. Khác với các mô hình đơn lẻ, MAS cho phép tự động hóa toàn bộ quy trình công việc bằng cách điều phối các tác nhân thực hiện các nhiệm vụ khác nhau một cách nhịp nhàng. Thị trường tác nhân AI tự chủ dự báo sẽ đạt quy mô 8,5 tỷ USD vào năm 2026 và có thể lên tới 45 tỷ USD vào năm 2030 nếu các doanh nghiệp giải quyết tốt bài toán về khả năng tương tác và quản trị hành vi của tác nhân. Xu hướng này đánh dấu sự chuyển dịch từ việc dùng AI như một công cụ hỗ trợ sang một động cơ điều phối thông minh trong doanh nghiệp.

5. Mô hình ngôn ngữ chuyên biệt: Tối ưu hóa độ chính xác và tính tuân thủ cho các lĩnh vực đặc thù

Thay vì phụ thuộc vào các mô hình ngôn ngữ lớn (LLM) tổng quát, các doanh nghiệp đang hướng tới mô hình ngôn ngữ chuyên biệt (DSLMS) được đào tạo hoặc tinh chỉnh trên các tập dữ liệu chuyên biệt của từng ngành như pháp lý, lâm sàng hoặc công nghiệp. DSLMS mang lại độ chính xác cao hơn, hiểu rõ các thuật ngữ kỹ thuật và ngữ cảnh đặc thù, đồng thời giảm chi phí vận hành và tăng cường khả năng quản trị. Đối với các tổ chức đang số hóa môi trường pháp lý, DSLMS giúp xây dựng các hệ thống AI không chỉ xử lý thông tin mà còn hiểu logic đằng sau các quy



Năm 2026 vẫn là cuộc đua tranh mạnh mẽ xung quanh trí tuệ nhân tạo.

định, hỗ trợ đưa ra các quyết định có tính minh bạch và có thể kiểm toán. Điều này giúp các doanh nghiệp biến sự tuân thủ thành một chất xúc tác cho đổi mới sáng tạo.

6. Trí tuệ nhân tạo vật lý: Khi trí tuệ kỹ thuật số làm chủ các thực thể cơ khí trong thế giới thực

AI vật lý đưa trí thông minh vào thế giới thực, vận hành các robot, máy bay không người lái và máy móc thông minh có khả năng cảm nhận, quyết định và hành động tự chủ. Các ví dụ thực tế bao gồm việc Amazon triển khai hơn một triệu robot trong kho bãi hoặc BMW vận hành các nhà máy nơi xe tự lái chạy qua các tuyến sản xuất dài hàng km. Sự hội tụ này tạo ra nhu cầu lớn về các bộ kỹ năng liên ngành mới giữa công nghệ thông tin và kỹ thuật cơ khí. Đến năm

2030, doanh số robot công nghiệp mới hàng năm có thể tăng gấp đôi lên mức một triệu đơn vị, thúc đẩy bởi sự thiếu hụt lao động và sự phát triển vượt bậc của các mô hình AI nền tảng chuyên biệt cho vật lý.

7. An ninh mạng tiên phong: Chủ động dự báo và vô hiệu hóa các mối đe dọa trước khi cuộc tấn công bắt đầu

An ninh mạng đang chuyển dịch từ trạng thái phòng thủ phản ứng sang dự báo chủ động bằng cách sử dụng AI để phân tích hành vi và vô hiệu hóa các mối đe dọa trước khi chúng gây ra tác động. Phương pháp này sử dụng các kỹ thuật lừa đảo (deception) và tự động hóa để ngăn chặn các cuộc tấn công hoạt động ở tốc độ máy. Đến năm 2030, các giải pháp an ninh mạng tiên phong dự kiến sẽ chiếm một nửa tổng chi



tiêu cho bảo mật toàn cầu. Đây là một sự tái cấu trúc cần thiết khi các mối đe dọa AI đang làm ngán lại “cửa sổ relevance” của các biện pháp bảo vệ truyền thống.

8. Truy xuất nguồn gốc kỹ thuật số: Thiết lập lòng tin thông qua việc xác thực nguồn gốc nội dung và dữ liệu

Trong kỷ nguyên của nội dung do AI tạo ra và các chuỗi cung ứng kỹ thuật số phức tạp, việc xác minh nguồn gốc và tính xác thực của dữ liệu trở nên tối quan trọng. Digital provenance sử dụng các cơ sở dữ liệu xác thực, hình mờ kỹ thuật số (watermarks) và hóa đơn vật liệu phần mềm (SBOMs) để theo dõi lịch sử và tính toàn vẹn của thông tin. Gartner cảnh báo rằng, các tổ chức không đầu tư vào công nghệ này có thể đối mặt với rủi ro pháp lý và các khoản phạt lên tới hàng tỷ USD vào năm 2029. Khả năng chứng minh nguồn gốc dữ liệu không chỉ là yêu cầu tuân thủ mà còn là một tài sản cạnh tranh về lòng tin đối với khách hàng.

9. Nền tảng an ninh trí tuệ nhân tạo: Quản trị rủi ro và bảo vệ toàn diện hệ sinh thái trí tuệ nhân tạo doanh nghiệp

Nền tảng an ninh AI (AISPs) cung cấp khả năng hiển thị và bảo vệ tập trung cho tất cả các hệ thống AI, bao gồm cả dịch vụ của bên thứ ba và các ứng dụng tự xây dựng. Các nền tảng này bảo vệ chống lại các rủi ro đặc thù của AI như tiêm mã độc vào câu lệnh (prompt injection), rò rỉ dữ liệu và các tác nhân AI hoạt động sai lệch. Đến năm 2028, hơn một nửa số doanh nghiệp sẽ dựa vào các nền tảng an ninh AI để bảo vệ các khoản đầu tư công nghệ của mình. Khi AI trở nên quan trọng đối với nhiệm vụ của tổ chức, rủi ro mô hình và chuỗi cung ứng AI sẽ trở thành mối quan tâm hàng đầu của các hội đồng quản trị.

10. Nội địa hóa hạ tầng số: Tái định vị hạ tầng kỹ thuật số để đảm bảo chủ quyền và khả năng phục hồi

Nội địa hóa hạ tầng số (Geopatriation) là xu hướng chuyển dịch các khối lượng công việc kỹ thuật số từ các đám mây công cộng toàn cầu sang các môi trường có chủ quyền hoặc khu vực để duy trì quyền kiểm soát dữ liệu và tuân thủ các quy định quốc gia. Động lực của xu hướng này là sự gia tăng rủi ro địa chính trị và

nhu cầu về sự ổn định của chuỗi cung ứng công nghệ. Dự kiến đến năm 2030, hơn 75% các doanh nghiệp tại châu Âu và Trung Đông sẽ thực hiện nội địa hóa các khối lượng công việc của họ. Điều này buộc các doanh nghiệp phải xem xét lại các hợp đồng đám mây toàn cầu và cấu trúc lại hệ thống để có khả năng phục hồi theo từng khu vực.

Sự hội tụ và những thách thức thực thi

Trong năm 2026, chìa khóa thành công của một doanh nghiệp không nằm ở việc sở hữu công nghệ đắt tiền nhất, mà ở quyết tâm thiết kế lại toàn bộ quy trình vận hành thay vì chỉ dùng AI để tự động hóa những cách làm cũ vốn đã không hiệu quả. Nếu tổ chức chỉ cố gắng “số hóa” những quy trình lỗi, họ sẽ chỉ nhận lại những sai lầm ở tốc độ nhanh hơn; thay vào đó, họ cần dũng cảm thực hiện một cuộc “đại tái thiết” để trở thành một tổ chức vận hành dựa trên nền tảng AI.

Sự phát triển hiện nay mang tính cộng hưởng mạnh mẽ (multiplicative) tương tự như một chiếc “bánh đà” tự vận hành: Công nghệ tiên tiến tạo ra nhiều ứng dụng thực tế, các ứng dụng này sinh ra dữ liệu khổng lồ, dữ liệu lại thu hút thêm vốn đầu tư để nâng cấp hạ tầng và hạ tầng tốt lại quay lại thúc đẩy công nghệ tiến xa hơn với chi phí thấp hơn. Đồng thời, trọng tâm của thế giới đang dịch chuyển từ việc “dạy” AI học (huấn luyện) sang việc đưa AI vào làm việc thực tế (thực thi/suy luận). Dự báo vào năm 2026, các hoạt động chạy mô hình AI để phục vụ người dùng sẽ chiếm tới 2/3 tổng công suất tính toán trên toàn cầu.

Tuy nhiên, khoảng cách giữa việc thử nghiệm và sản xuất thực tế vẫn còn lớn, khi chỉ có 11% các tổ chức hiện có các tác nhân AI đang hoạt động thực sự trong sản xuất. Các rào cản về hạ tầng, chi phí mã thông báo (tokens) và sự thiếu hụt tài năng đang là những điểm nghẽn cần giải quyết. Cuối cùng, niềm tin sẽ là “người gác cổng” cho sự chấp nhận công nghệ; các doanh nghiệp phải chứng minh được tính minh bạch, công bằng và trách nhiệm trong mọi mô hình AI mà họ triển khai.

MH (tổng hợp từ các báo cáo công nghệ quốc tế)