IBM Security

IBM

Vượt qua thách thức về bảo vệ dữ liệu ở khắp mọi nơi

Giữ an toàn cho dữ liệu nhạy cảm trong thời đại Điện toán Đám mây

Nhấp vào hình tròn để truy cập chương

1

Triển khai môi trường đám mây

Các tổ chức đang nhanh chóng chuyển sang công nghệ đám mây thông qua việc tận dụng cơ sở hạ tầng dưới dạng dịch vụ (IaaS), phần mềm dưới dạng dịch vụ (SaaS) và nền tảng dưới dạng dịch vụ (PaaS) như những cách thức mới để tối ưu hóa hoạt động sản xuất kinh doanh cho dù các môi trường này mang đến nhiều rủi ro mới cho dữ liệu nhạy cảm.

2

Thách thức về bảo mật đám mây

Triển khai đám mây đồng nghĩa với việc dữ liệu nhạy cảm được giữ ở những nơi bạn không thể kiểm soát và được bên thứ ba quản lý mà các bên này có thể sở hữu quyền truy cập không giới hạn vào dữ liệu đó.

3

Thách thức về tổ chức

Những thách thức khi bảo vệ dữ liệu trong đám mây bao gồm đảm bảo sự tuân thủ, giám sát công cụ kiểm soát truy cập, đảm bảo quyền riêng tư, cải thiện năng suất, và xử lý các lỗ hổng - tất cả những thách thức này song hành cùng quá trình sử dụng dữ liệu tại cơ sở và dữ liệu dựa trên đám mây để phát triển doanh nghiệp.

4

Phương pháp bảo vệ dữ liệu

Các công nghệ bảo mật và bảo vệ dữ liệu cần vận hành trong nhiều môi trường (vật lý, đám mây và lai) cùng một lúc. Giải pháp bảo mật dữ liệu của bạn phải được tự động hóa, có khả năng linh động và tùy ứng, đồng thời có khả năng mã hóa thống nhất và linh hoạt.

5

Kết luận

Trong khi điện toán đám mây trở nên phổ biến, các quy tắc cơ bản về bảo mật vẫn không thay đổi: bảo mật, bảo vệ dữ liệu và hỗ trợ sự tuân thủ.

1.1 Triển khai môi trường đám mây

Chỉ cách đây vài năm, nhiều tổ chức đã chuyển sang môi trường đám mây riêng để giúp nâng cao tính linh hoạt và kiểm soát chi phí - chủ yếu vì môi trường đám mây công cộng thời ấy chưa hoàn thiện, thiếu khả năng kiểm soát và chưa phổ biến. Tuy nhiên, ngày nay, quyết định "đi lên mây" không còn bị bó hẹp nữa mà có rất nhiều lựa chọn với các mô hình triển khai (công cộng, riêng tư và lai) cùng các loại dịch vụ khác nhau, bao gồm IaaS, PaaS và SaaS.

Với nhiều tùy chọn chi tiết hơn, việc triển khai đám mây đã được phân khúc theo ngành nghề kinh doanh chứ không hẳn là một quyết định về CNTT được chuẩn hóa. Và mặc dù danh sách các tùy chọn mới về đám mây rất dài nhưng hầu hết doanh nghiệp sẽ áp dụng môi trường lai và kết hợp để tận dụng những khoản đầu tư hiện có trong các khung chính, cơ sở dữ liệu tại cơ sở, hệ thống phân phối dữ liệu lớn, hệ thống tệp, v.v..[1]

Đám mây riêng là cơ sở hạ tầng CNTT được vận hành cho riêng một tổ chức và do nội bộ tổ chức hoặc bên thứ ba quản lý. Với đám mây riêng, các tổ chức kiểm soát được toàn bộ hệ thống phần mềm cũng như nền tảng ngầm, từ cơ sở hạ tầng phần cứng tới các công cụ đo lường. Dịch vụ đám mây riêng dành cho các đơn vị kinh doanh của một doanh nghiệp sử dụng (hoặc chỉ được chia sẻ với đối tác của doanh nghiệp).[1] Tuy nhiên, khi đưa tải làm việc vào đám mây riêng, việc bảo mật dữ liệu trong môi trường ảo thậm chí còn trở nên quan trọng hơn, đặc biệt là khi kết hợp tải làm việc c ở các mức độ tin cậy khác nhau để chạy trên cùng một phần cứng vật lý. Nghiên cứu của công ty Gartner cho thấy các tổ chức sẽ tiếp tục sử dụng và đầu tư nhiều vào điện toán đám mây riêng. Tuy nhiên, gần như tất cả các doanh nghiệp mà Gartner khảo sát đều muốn sử dụng mô hình đám mây lai - mô hình có cả yếu tố đám mây riêng và công cộng. Các doanh nghiệp đang triển khai tùy chọn điện toán đám mây công cộng dưới dạng chìa khóa trao tay để cung cấp dịch vụ nhanh chóng, thông suốt hơn và để tăng cường độ nhạy bén trong kinh doanh cũng như khuyến khích đổi mới. Điện toán đám mây công cộng đóng vai trò then chốt trong sự đổi mới và do vậy, được dự báo sẽ có mức tăng trưởng thường niên là 15,2% trong suốt năm 2019.[1]

Khi nói tới môi trường đám mây, cho dù là đám mây công cộng hay riêng tư thì các công cụ bảo mật và bảo vệ dữ liệu phải bảo vệ được dữ liệu nhạy cảm và hỗ trợ cho các yêu cầu không ngừng gia tăng trong vấn đề tuân thủ từ phía chính phủ và ngành.

1.2 Triển khai môi trường đám mây

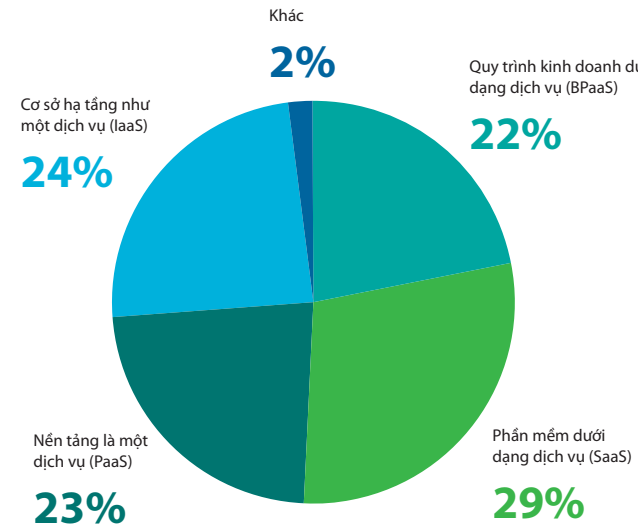
Các loại dịch vụ phổ biến nhất là IaaS, PaaS và SaaS. Cách dễ nhất để hình dung sự khác biệt giữa các loại dịch vụ này là xem xét hệ thống CNTT của bạn. Ở lớp dưới cùng, bạn có cơ sở hạ tầng - bao gồm phần cứng, máy chủ và mạng - hoạt động như nền tảng CNTT của tổ chức. Phía trên cơ sở hạ tầng này, bạn có nền tảng phần mềm hoặc phần mềm trung gian cung cấp công cụ cần thiết cho nhà phát triển triển khai các ứng dụng kinh doanh. Và ở trên cùng, bạn có các ứng dụng kinh doanh giao tiếp với nhân viên nội bộ và khách hàng.

IaaS cho phép tổ chức duy trì các nền tảng phần mềm, phần mềm trung gian vật lý và các ứng dụng kinh doanh hiện có nhưng thuê ngoài việc quản lý cơ sở hạ tầng bên dưới của tổ chức. Các công ty làm như vậy với ý định tận dụng nhanh lợi thế của đám mây, đồng thời giảm thiểu các tác động và vẫn có thể thể sử dụng những khoản đầu tư hiện hữu.

PaaS cho phép các công ty thuê ngoài cơ sở hạ tầng cũng như phần mềm trung gian hoặc phần mềm. Điều này loại bỏ gánh nặng lớn cho công ty xét ở góc độ CNTT và cho phép công ty tập trung vào phát triển ứng dụng kinh doanh đổi mới.

SaaS là tùy chọn đặc biệt nhất. Loại dịch vụ này thuê ngoài toàn bộ CNTT và cho phép tổ chức tập trung hơn vào thế mạnh chính của mình (ví dụ: dịch vụ y tế, tài chính) thay vì dành quá nhiều thời gian và tiền đầu tư cho công nghệ, lĩnh vực có thể dành cho các chuyên gia công nghệ.

Với mỗi bước, từ IaaS đến PaaS, đến SaaS, các tổ chức đều từ bỏ một mức độ kiểm soát nào đó đối với các hệ thống lưu trữ, quản lý và phân phối dữ liệu nhạy cảm của họ. Điều này cho thấy sự nâng cao sự tin tưởng đối với bên thứ ba, nhưng đồng thời cũng tăng mức độ rủi ro.



Hình 1: Câu hỏi thăm dò ý kiến: “Ngân sách hiện đang phân bổ cho các dịch vụ đám mây ‘công cộng’ được phân chia như thế nào giữa các loại đám mây sau?”

Nguồn: Ed Anderson và Sid Nag, “Xu hướng thị trường: Xu hướng sử dụng đám mây thiên về đám mây công cộng có đặc tính lai” Gartner, ngày 4/8/2016. ID: G00294424.

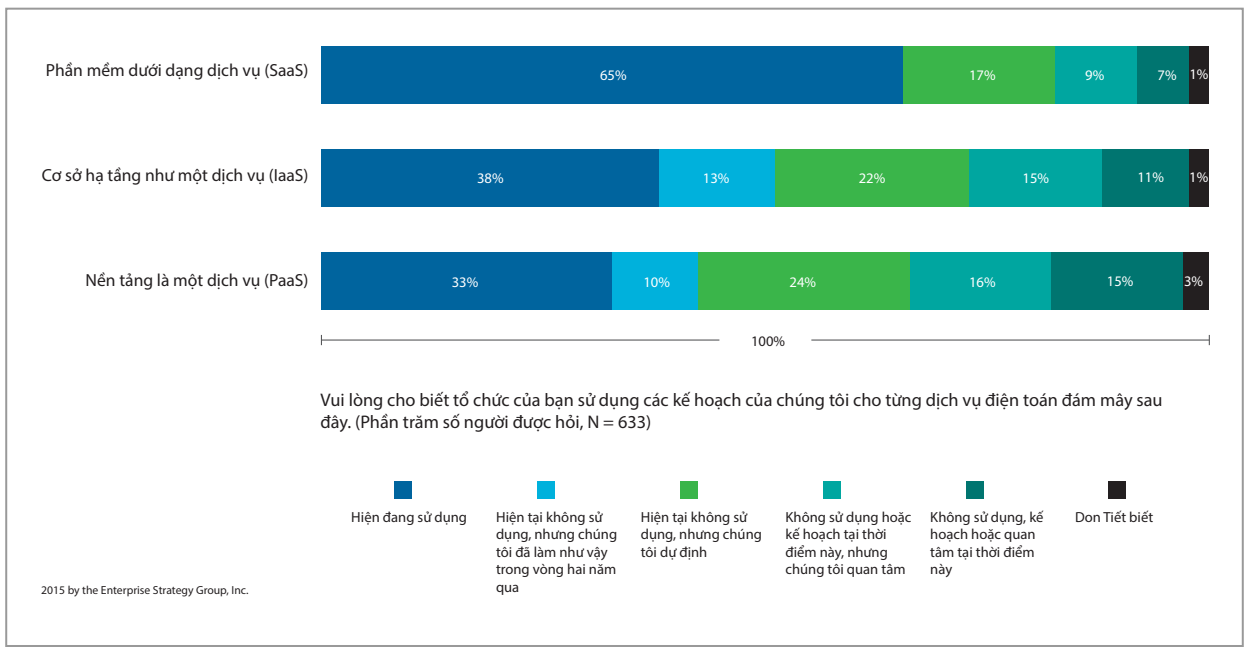
1.3 Triển khai môi trường đám mây

"Sử dụng đám mây" có rất nhiều lựa chọn. Một nghiên cứu trên hơn 600 người ra quyết định về CNTT của doanh nghiệp cho thấy phần lớn các hãng được khảo sát đều đã sử dụng ít nhất một vài ứng dụng SaaS; chưa đầy 20% người trả lời khảo sát không có kế hoạch hoặc không quan tâm tới việc thuê SaaS.

Việc triển khai PaaS đòi hỏi mức độ cam kết cao hơn về điện toán và lưu trữ dữ liệu ở bên ngoài cơ sở, do đó, có thể hiểu vì sao lựa chọn này đứng sau các ứng dụng đám mây từng phần, nhưng 67% người trả lời khảo sát đã sử dụng, từng sử dụng hoặc có kế hoạch sử dụng PaaS.

Việc sử dụng cơ sở hạ tầng đám mây - IaaS - giúp chuyển gánh nặng cài đặt và duy trì cơ sở hạ tầng vật lý từ doanh nghiệp sang một nhà cung cấp chuyên biệt và số liệu thống kê về IaaS nằm giữa các số liệu thống kê về PaaS và SaaS. Vào thời điểm tiến hành khảo sát này, 73% người trả lời đã sử dụng hoặc có kế hoạch sử dụng hình thức cơ sở dữ liệu đám mây nào đó hoặc đã thử nghiệm hình thức này.

Thách thức về bảo vệ dữ liệu đám mây ảo và riêng



2.1 Thách thức về bảo mật đám mây

2

Đám mây đặc biệt phù hợp với việc lưu trữ dữ liệu dâu dài ở cấp độ doanh nghiệp - với quy mô kinh tế về cả trang thiết bị và quản trị, có thể khiến các trung tâm dữ liệu dựa trên đám mây thành nơi lưu trữ thông minh hơn để lưu trữ thông tin quan trọng trong kinh doanh so với một dãy máy chủ đặt trong hội sảnh. Đó là ngay cả khi chi phí lưu trữ giảm, nhưng chi phí từ việc sử dụng theo nhu cầu kinh doanh ngày càng nhiều cùng chi phí nhân sự quản lý lưu trữ tiếp tục tăng. Tuy nhiên, mặc dù việc chuyển công việc lưu trữ dữ liệu sang tay các quản trị viên chuyên trách có thể giúp tiết kiệm tiền bạc và thời gian, nhưng điều này cũng có thể đặt ra những thử thách bảo mật lớn và có thể gây ra những mức độ rủi ro mới.

Điều quan trọng là phải nhận ra rằng bất kỳ mô hình triển khai hay loại dịch vụ nào thì những nguyên tắc cơ bản về bảo mật dữ liệu vẫn không được thay đổi. Điều thực sự thay đổi là dữ liệu nhạy cảm của bạn giờ nằm ở nhiều nơi, cả bên trong lẫn bên ngoài bốn bức tường của công ty bạn. Điều này có nghĩa là các công cụ kiểm soát bảo mật cần song hành với dữ liệu của bạn. Khi đánh giá công nghệ bảo mật dữ liệu, hãy chọn các giải pháp hoạt động minh bạch và đồng thời trong nhiều môi trường. Hãy đảm bảo giải pháp bảo mật dữ liệu có tính chất động và thích ứng trên toàn bộ các môi trường để bạn không cần trang bị thêm công cụ bảo vệ dữ liệu bổ sung ngoài dự kiến.

Giữ dữ liệu an toàn trước mọi đối tượng và ở mọi nơi

Điều quan trọng nhất trong những thách thức này là rõ ràng: dữ liệu nhạy cảm giờ có ở khắp mọi nơi, cả bên trong lẫn bên ngoài tường lửa của bạn và đang được quản lý theo một cách nào đó bởi nhân viên của bạn cũng như bên thứ ba. Bạn không còn có thể bảo vệ dữ liệu nhạy cảm chỉ bằng cách đơn giản là khóa quyền truy cập mạng. Trên thực tế, bạn dựa vào mạng để truy cập và chia sẻ dữ liệu. Điều này đặt sự an toàn của dữ liệu vào trong tay của nhiều người hơn trước kia và nhiều người trong số đó không còn làm việc trực tiếp cho công ty bạn nữa. Nhìn chung, trong môi trường đám mây, nhà cung cấp dịch vụ đám mây (CSP) có khả năng truy cập dữ liệu nhạy cảm của bạn nên họ trở thành đối tượng mới trong các mối đe dọa nội bộ. Ngoài ra, tội phạm mạng biết rằng CSP lưu trữ khối lượng lớn dữ liệu quan trọng. Cả hai mối nguy này khiến các khả năng như mã hóa dữ liệu và giám sát hoạt động của dữ liệu trở thành một phần đặc biệt giá trị trong chiến lược bảo mật của bạn.

2.2 Thách thức về bảo mật đám mây

Khả năng di chuyển của dữ liệu là một lý do khiến việc lưu trữ trên đám mây trở thành một lựa chọn mang tính kinh tế để bắt đầu. Các chi phí về cơ sở hạ tầng (từ chi phí bất động sản tới chi phí năng lượng) thay đổi rất nhiều theo khu vực địa lý và thậm chí theo cả thời gian trong ngày. Tương tự, chi phí và hiệu quả của các loại phương tiện lưu trữ cũng khác nhau. Băng từ, đĩa quay và ổ đĩa trạng thái rắn đều là các phương tiện tiên tiến về dung lượng, tốc độ và tính tin cậy, và sự pha trộn mang tính kinh tế nhất của các công nghệ lưu trữ đối với một doanh nghiệp xác định có thể thay đổi nhanh chóng. Vì thế, với công nghệ lưu trữ trên đám mây, ngày mai, dữ liệu của bạn có thể hoạt động ở một nơi khác, trên phương tiện khác vị trí lưu trữ hôm nay. Điều này cũng đúng với công nghệ ảo. Không chỉ dữ liệu dựa trên đám mây mà cả tài nguyên điện toán dựa trên đám mây cũng có thể thay đổi - một cách rõ ràng và nhanh chóng - về cả vị trí lẫn nền tảng phần cứng.

Tính chất của công nghệ đám mây thay đổi đồng nghĩa với việc các phương pháp bảo mật để lưu trữ dựa trên đám mây cũng cần xử lý được các hình thức lưu trữ khác nhau. Phương pháp bảo mật của bạn cũng phải tính đến các bản sao, đến việc tạo bản sao lưu dài hạn hay bản sao tạm thời trong quá trình lưu chuyển dữ liệu. Để giải quyết những thách thức này, hãy chọn giải pháp đa nền tảng và sử dụng công nghệ mã hóa cao.

Ngay cả khi dữ liệu của bạn không được lưu trữ chủ yếu trên đám mây thì cả hình thức đưa dữ liệu đi ra ngoài và quay lại doanh nghiệp cũng như lộ trình của dữ liệu cũng đều là những mối lo ngại lớn. Ngay cả khi dữ liệu chủ yếu được mã hóa và có tường lửa bảo vệ tại cơ sở, nếu một phần dữ liệu bị lộ khi truyền đến một vị trí sao lưu bên ngoài cơ sở hoặc để cho một bên thứ ba xử lý thì dữ liệu nhạy cảm đó cũng chỉ an toàn như một liên kết yếu nhất trong chuỗi xử lý dữ liệu.

Để bảo vệ dữ liệu hiệu quả khi dữ liệu ở trên đám mây cần có cả các biện pháp phòng ngừa thụ động (như chặn quyền truy cập trên các cổng không được phê duyệt) và các biện pháp chủ động, như liên tục quét tìm các lượt truy cập dữ liệu đáng ngờ. Biện pháp chính trong số các biện pháp này mà bạn có thể áp dụng là tiến hành mã hóa dữ liệu nhạy cảm. Mặc dù các hệ thống phát hiện phần mềm độc hại hoặc phân tích hành vi được thiết kế nhằm tìm ra lượt truy cập đáng ngờ có thể giúp ngăn chặn hành vi vi phạm trong nội bộ hoặc bên ngoài đối với dữ liệu, công nghệ mã hóa - bản thân có các chức năng quý giá - giúp bảo vệ dữ liệu ở bất kỳ nơi nào dữ liệu tồn tại, dù dữ liệu có đang di chuyển hay không.

2.3 Thách thức về bảo mật đám mây

Các mối liên quan về quản trị và pháp lý
Thực tế về lưu trữ và điện toán dựa trên đám mây đồng nghĩa với việc bảo mật dữ liệu nhạy cảm trên các hệ thống đám mây và đám mây lai hiếm khi suôn sẻ như hy vọng của các quản trị viên. Công cụ bảo mật cung cấp giao diện thống nhất trên khắp các đầu cuối đám mây - từ trang trại máy chủ chuyên dụng bên ngoài cơ sở tới các máy ảo trong cơ sở hạ tầng của đám mây công cộng - là sự khởi đầu tốt để thực hiện lời hứa về việc quản trị hiệu quả từ xa.

Vấn đề quan trọng không kém nữa là các yêu cầu pháp lý và chủ quyền dữ liệu - nói cách khác đây là các quy tắc về bảo mật và bảo vệ dữ liệu khi dữ liệu nhạy cảm được lưu trữ vật lý tại một địa điểm cụ thể. Lưu trữ dữ liệu trong đám mây có thể dẫn tới việc lưu trữ dữ liệu nhạy cảm ở những nơi áp dụng các điều luật nghiêm ngặt hơn điều luật ở vị trí ban đầu của dữ liệu. Ví dụ: theo điều khoản trong Quy định bảo vệ dữ liệu chung của Liên minh châu Âu (GDPR), việc bảo vệ nghiêm ngặt hơn đối với các dữ liệu cá nhân của người dân ở quốc gia thuộc Liên minh châu Âu là điều bắt buộc. Những yêu cầu này áp dụng với cả các công ty nằm ở khu vực khác của thế giới nhưng nắm giữ và truy cập dữ liệu cá nhân của người dân tại Liên minh châu Âu.

Biết rõ ai đang truy cập dữ liệu của bạn: *IBM® Security Guardium® có thể giúp bảo mật cơ sở hạ tầng đám mây và đám mây lai bằng các công cụ giám sát và đánh giá có khả năng phát hiện ra các vấn đề bất thường và những lỗ hổng.*

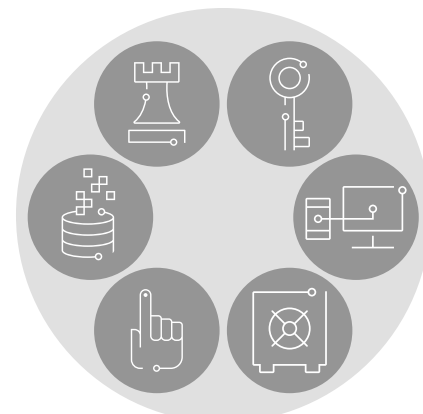
3.1 Thách thức về tổ chức

3

Các tổ chức vẫn gặp phải vô vàn thách thức khi cố gắng bảo vệ dữ liệu nhạy cảm và các quy định phức tạp là một lý do. Công ty Forrester chỉ ra rằng ngày nay, "hầu hết các kiến trúc sư doanh nghiệp và các chuyên gia bảo mật đều đang phải vật lộn với việc nâng cao tính bảo mật của dữ liệu hoặc đáp ứng các yêu cầu về tuân thủ do kho dữ liệu và khối lượng dữ liệu ngày càng gia tăng. Áp dụng các chính sách kiểm soát truy cập thống nhất trên khắp các cơ sở dữ liệu, kho dữ liệu, Hadoop, NoSQL và tệp đã trở thành một việc vô cùng thử thách."[2]

Công nghệ ảo có tiềm năng làm cho việc áp dụng các công cụ bảo mật và cơ chế tuân thủ trở nên dễ dàng hơn nhưng chỉ khi môi trường đám mây ảo hoặc riêng có thể hỗ trợ bảo vệ dữ liệu nhạy cảm bằng cách đáp ứng đồng bộ các yêu cầu tuân thủ, nhu cầu kiểm soát truy cập, yêu cầu về quyền riêng tư, yêu cầu về lỗ hổng và nhu cầu về năng suất.

Thách thức về bảo vệ dữ liệu đám mây ảo và riêng



Tuân thủ
Năng suất
Kiểm soát truy cập
Lỗ hổng
Quyền riêng tư

Hình 2: Bảo vệ dữ liệu lưu trữ trên đám mây vẫn yêu cầu các quản trị viên chú ý tới các khía cạnh bảo mật, từ bảo mật và quyền riêng tư tới việc tuân thủ quy định trên một số miền.

3.2 Thách thức về tổ chức

Tuân thủ

Hãy nghĩ về nơi mà dữ liệu nhạy cảm nằm trong môi trường đám mây. Xác định, phân loại dữ liệu nhạy cảm và thiết lập chính sách sử dụng dữ liệu đó là điều quan trọng, cho dù trong môi trường đám mây công cộng hay đám mây riêng. Nếu dữ liệu nằm trên đám mây công cộng, bạn cần tìm hiểu cách nhà cung cấp cơ sở hạ tầng đám mây lên kế hoạch bảo vệ dữ liệu nhạy cảm của bạn như thế nào.

Trong cả hai trường hợp thì việc tìm hiểu dữ liệu nằm ở đâu, có những miền thông tin gì đang tồn tại và những vấn đề này liên quan như thế nào trong toàn bộ doanh nghiệp sẽ giúp tổ chức xác định chính sách đúng đắn để bảo mật và mã hóa dữ liệu đó và để chứng minh sự tuân thủ với các quy định như Sarbanes-Oxley (SOX), Tiêu chuẩn bảo mật dữ liệu trong ngành thẻ thanh toán (PCI DSS), Giao thức tự động hóa nội dung bảo mật (SCAP), Đạo luật quản lý bảo mật thông tin liên bang (FISMA), Đạo luật về khả năng di chuyển và trách nhiệm giải trình thông tin bảo hiểm y tế (HIPAA) và Đạo luật công nghệ thông tin y tế (HITECH). Các quy định về tuân thủ liên tục xuất hiện và tổ chức vẫn phải chịu trách nhiệm giải trình ngay cả khi dữ liệu di chuyển lên đám mây.

Quyền riêng tư

Một thách thức nữa của quản trị viên quyền truy cập dữ liệu là đảm bảo chỉ những người có lý do công việc hợp lý mới được quyền truy cập thông tin cá nhân. Ví dụ: các bác sĩ cần xem thông tin nhạy cảm như dữ liệu về triệu chứng và tiên lượng của bệnh nhân, trong khi đó, một nhân viên lập hóa đơn chỉ cần biết số bảo hiểm và địa chỉ lập hóa đơn của bệnh nhân.

3.3 Thách thức về tổ chức

Kiểm soát truy cập

Tội phạm mạng là những kẻ có ý đồ không trung thực và muốn phá hoại. Chúng có thể là những nhà khoa học máy tính gian xảo cố gắng thể hiện hay đưa ra một tuyên bố chính trị, hoặc cũng có thể là những kẻ xâm nhập rắn mặt, có tổ chức. Các quốc gia nước ngoài đã tài trợ cho tin tặc thu thập thông tin tình báo từ các tổ chức chính phủ. Thậm chí, tin tặc có thể là các nhân viên bất mãn. Việc vi phạm cũng có thể do vô tình - ví dụ khi đặt sai quyền trên bảng cơ sở dữ liệu hoặc khi thông tin đăng nhập của nhân viên bị xâm hại. Các phương thức thực hiện tốt nhất cho thấy nên cấp "đặc quyền thấp nhất có thể" cho cả người dùng cuối được ưu tiên và người dùng cuối bình thường để giảm thiểu việc lạm dụng đặc quyền và giảm thiểu lỗi. Tổ chức nên bảo vệ dữ liệu khỏi bị tấn công cả từ bên trong lẫn bên ngoài trong môi trường vật lý, môi trường đám mây ảo và riêng.

Biện pháp phòng vệ từ vòng ngoài là quan trọng nhưng bảo vệ chính dữ liệu nhạy cảm cũng không kém phần quan trọng. Nếu vòng ngoài bị xâm phạm, dữ liệu nhạy cảm cần có sẵn tính an toàn (và kẻ cắp không thể sử dụng được) để giảm thiểu ảnh hưởng của việc xâm phạm và đảm bảo tin tặc không thể truy cập tự do. Các biện pháp phòng vệ cần có giải pháp bảo mật dữ liệu theo lớp để quản trị viên có thể tìm hiểu điều gì đang xảy ra bên trong đám mây riêng - ví dụ: bằng cách tìm hiểu mô hình truy cập dữ liệu và hành vi của người dùng được ưu tiên.

Thách thức ở đây là đưa ra các biện pháp bảo vệ dữ liệu và quyền truy cập thích hợp trong khi vẫn đáp ứng yêu cầu công việc và đảm bảo dữ liệu được quản lý trên cơ sở "cần biết" - dù dữ liệu nằm ở đâu.

Năng suất

Chính sách bảo mật và quyền riêng tư cần tạo điều kiện và hỗ trợ cho các hoạt động kinh doanh chứ không được gây cản trở. Những chính sách này cần được đưa vào các hoạt động hàng ngày và vận hành thông suốt trong và trên khắp tất cả các môi trường - môi trường đám mây riêng, môi trường đám mây công cộng, môi trường tại cơ sở và môi trường lai - mà không ảnh hưởng tới năng suất của người dùng. Ví dụ: khi đám mây riêng được triển khai để hỗ trợ thử nghiệm ứng dụng, hãy cân nhắc sử dụng công nghệ mã hóa hoặc số hóa thẻ để giảm rủi ro lộ thông tin nhạy cảm đó.

3.4 Thách thức về tổ chức

Lỗ hổng

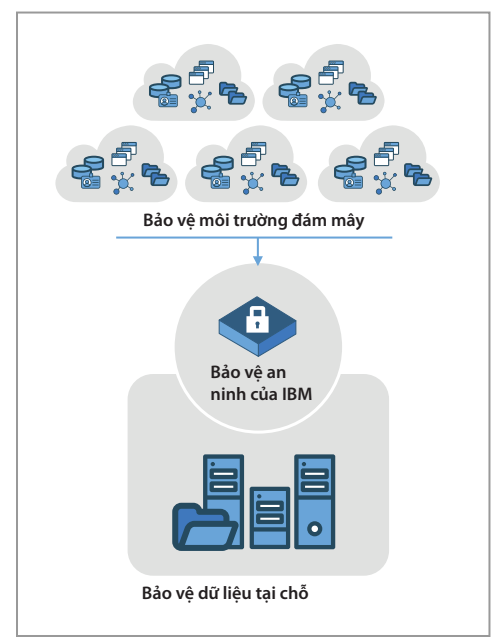
Ngày nay, các tổ chức áp dụng nhiều công nghệ bảo mật đa dạng để bảo vệ dữ liệu của doanh nghiệp và hỗ trợ vấn đề tuân thủ. Nhưng số lượng lỗ hổng trong kho dữ liệu là vô vùng lớn và tội phạm có thể khai thác ngay cả những cơ hội nhỏ nhất. Việc hiểu các lỗ hổng từ tất cả các góc độ và phát triển phương pháp xử lý chúng là điều quan trọng. Những lỗ hổng thông thường bao gồm: thiếu bản vá lỗi, cấu hình sai và các cài đặt hệ thống mặc định. Vấn đề phức tạp này ngày càng khó theo dõi và quản lý nhất là khi các kho dữ liệu được ảo hóa.

Khi các tổ chức chuyển sang đám mây riêng cũng như công cộng chẳng hạn thì những giải pháp này không phải lúc nào cũng phù hợp. Ngoài ra, một số phương pháp mã hóa chỉ đi với một phần cứng hoặc tài nguyên mạng cụ thể. Trong môi trường đám mây, quản trị viên không thể trông cậy vào quyền truy cập cơ sở hạ tầng phần cứng ở cấp thấp.

Một vấn đề nữa thường phát sinh khi sử dụng đám mây riêng để thử nghiệm hoặc phát triển ứng dụng. Đó là các cơ sở dữ liệu mới thường xuyên được tạo ra và ngừng hoạt động. Dữ liệu cần được bảo vệ vì những cơ sở dữ liệu này được tạo ra theo cơ chế động để hỗ trợ việc thử nghiệm và phát triển. Phương pháp bảo mật dữ liệu có thể điều chỉnh quy mô dành cho những môi trường đám mây riêng như vậy đồng nghĩa với việc khi cơ sở dữ liệu mới này hình thành, chúng sẽ được tự động phát hiện và dữ liệu nằm trong đó được tự động phân loại, giám sát và bảo vệ.

Cuối cùng, hãy nghĩ về việc sử dụng các công cụ tự chế đang được sử dụng hiện nay để bảo mật dữ liệu - ví dụ: quy trình che dấu dữ liệu hoặc đoạn mã giám sát hoạt động của cơ sở dữ liệu. Có cần thay đổi gì về mã hóa để làm cho các công cụ này hoạt động trên cơ sở dữ liệu ảo không? Có thể, bạn cần một khoản đầu tư lớn để cập nhật những giải pháp tự chế này - nhưng sau đó, bạn vẫn phải đối mặt với những thử thách lớn. Tốt nhất là khi thêm cơ sở dữ liệu mới hoặc nguồn dữ liệu khác, các quy trình và thủ tục bảo mật cần được tiến hành mà không có sự can thiệp thủ công. Tóm lại, các chiến lược bảo mật cần được tích hợp vào từng thành phần của bất kỳ môi trường đám mây nào.

Phương pháp bảo vệ dữ liệu



4.1 Phương pháp bảo vệ dữ liệu

Các tổ chức nên tìm cách tập trung hóa các công cụ kiểm soát bảo mật và bảo vệ dữ liệu trong môi trường đám mây riêng và công cộng cũng như trong phần còn lại của doanh nghiệp và đảm bảo tách biệt các nhiệm vụ để quản trị viên dữ liệu cũng không trở thành quản trị viên hoặc kiểm toán viên bảo mật. Các yếu tố then chốt trong chiến lược đám mây bảo mật bao gồm:

- Tìm hiểu nơi tồn tại dữ liệu nhạy cảm và ai có quyền truy cập dữ liệu đó. Tổ chức không thể bảo vệ dữ liệu nhạy cảm bằng mã hóa hoặc áp dụng các công cụ kiểm soát truy cập cứng rắn trừ khi họ biết nơi có dữ liệu nhạy cảm và dữ liệu đó liên quan như thế nào trong toàn bộ doanh nghiệp.
- Bảo vệ dữ liệu nhạy cảm có cấu trúc và không có cấu trúc, trực tuyến và ngoại tuyến, bằng các công nghệ phù hợp và thiết lập những yêu cầu truy cập thích hợp.
- Bảo vệ dữ liệu trước khi sản xuất, trong môi trường phát triển, thử nghiệm và đảm bảo chất lượng.
- Giám sát liên tục và an toàn quyền truy cập dữ liệu nhạy cảm - dù dữ liệu nằm ở đâu.
- Chứng minh sự tuân thủ để vượt qua các yêu cầu của kiểm toán bằng các báo cáo xây dựng sẵn cho kiểm toán viên và bằng quy trình làm việc tự động để bạn có thể thu được báo cáo phù hợp cho đúng người vào đúng thời điểm để phê duyệt.

Các chiến lược bảo vệ toàn diện dành cho tất cả môi trường đám mây và đám mây lai nên đưa ra cảnh báo về hành vi đáng ngờ cho quản trị viên bảo mật. Tổ chức cũng nên cân nhắc sử dụng những giải pháp bảo mật dữ liệu hỗ trợ sự tuân thủ tự động giúp đơn giản hóa quá trình tuân thủ.

Quy trình bảo mật dữ liệu cho môi trường đám mây cần liên tục theo dõi dữ liệu và cung cấp thông tin chi tiết về ai đang truy cập dữ liệu trên khắp các ứng dụng, cơ sở dữ liệu, kho, lượt chia sẻ tệp, môi trường dữ liệu lớn, v.v.. Phương pháp như vậy có thể giúp đảm bảo việc bảo vệ 360 độ cho dữ liệu nhạy cảm của tổ chức bất kể dữ liệu nằm ở đâu.

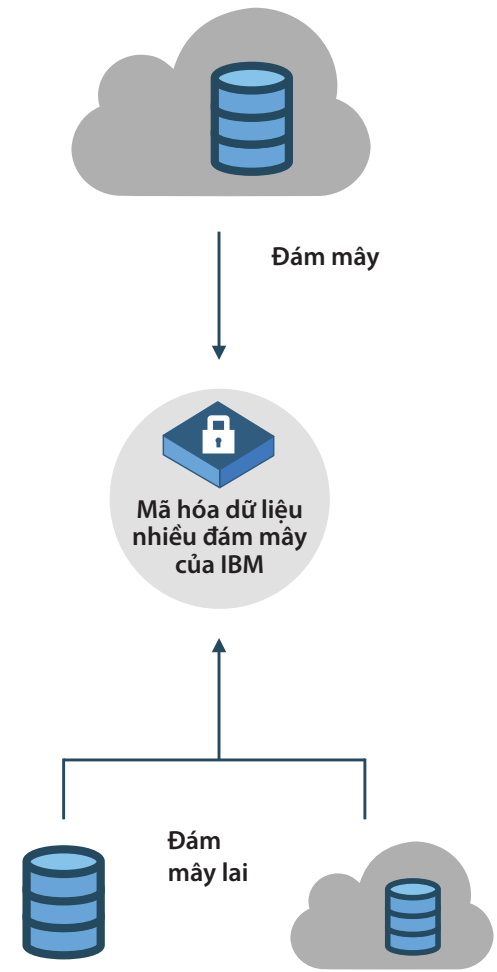
4.2 Phương pháp bảo vệ dữ liệu

Gánh nặng pháp lý của đối tượng nắm giữ dữ liệu (cũng như rủi ro vi phạm) có thể khiến những doanh nghiệp đang cân nhắc sử dụng bộ nhớ dựa trên đám mây mới hoặc mở rộng phải thận trọng. Công nghệ mã hóa cao là câu trả lời hiển nhiên nhất cho thách thức bảo mật dữ liệu nhạy cảm, bên trong hoặc bên ngoài cơ sở, nhưng việc mã hóa đặt ra các vấn đề phức tạp về đảm bảo khả năng di chuyển và truy cập. Dữ liệu chỉ có giá trị tốt nếu các khóa bảo vệ dữ liệu có tính bảo mật và đáng tin cậy. Những khóa này được sao lưu như thế nào? Liệu dữ liệu có thể lưu chuyển một cách minh bạch giữa các nhà cung cấp dịch vụ đám mây hoặc chia sẻ giữa các bộ nhớ dựa trên đám mây và bộ nhớ cục bộ không?

IBM Multi-Cloud Data Encryption bảo vệ dữ liệu đám mây (và đám mây lai), đồng thời chú trọng tới các yêu cầu về khả năng di chuyển và sự tuân thủ. Để giúp các khóa mã hóa được tiếp cận và cung cấp một cách an toàn, có thể tích hợp khóa bảo mật vào trình quản lý khóa nâng cao.

Ngoài ra, IBM Security Key Lifecycle Manager, dựa vào bộ nhớ được mã hóa dựa trên phần cứng, có thể giúp các khách hàng có yêu cầu bảo vệ dữ liệu nghiêm ngặt hơn đơn giản hóa và tập trung hóa việc quản lý khóa mã hóa mà không lo lộ dữ liệu trong môi trường đám mây ảo.

Quản lý khóa là yếu tố then chốt trong môi trường mã hóa bảo mật.



5.1 Kết luận

Để đảm bảo dữ liệu được bảo vệ trong môi trường ảo và đám mây, tổ chức cần tìm hiểu dữ liệu gì sẽ đi vào những môi trường ấy, có thể giám sát quyền truy cập vào dữ liệu này như thế nào, có những loại lỗ hổng nào tồn tại và làm cách nào có thể chứng minh sự tuân thủ. Các giải pháp bảo vệ cần được tích hợp vào môi trường đám mây từ đầu với mục tiêu đầu tiên là giúp tổ chức chứng minh sự tuân thủ.

Khi chọn giải pháp bảo mật và bảo vệ dữ liệu, hãy chọn những giải pháp có thể điều chỉnh quy mô và mở rộng trên khắp cơ sở hạ tầng CNTT để bảo vệ môi trường vật lý, ảo và đám mây khỏi những cuộc tấn công độc hại từ bên ngoài, khỏi những hành vi gian lận, truy cập trái phép và vi phạm trong nội bộ. Những giải pháp này phải hoạt động được trong môi trường đám mây mà không cần bất kỳ việc thiết lập, cấu hình đặc biệt nào hay bất kỳ chi phí bổ sung nào. Phương pháp như vậy sẽ tạo ra nền tảng hiệu quả cho việc bảo mật dữ liệu và đảm bảo quyền riêng tư, giúp quản lý chi phí bằng cách giảm tài nguyên bảo mật dữ liệu và nâng cao tính nhạy bén, linh hoạt nhờ việc tự bảo mật và đảm bảo quyền riêng tư.

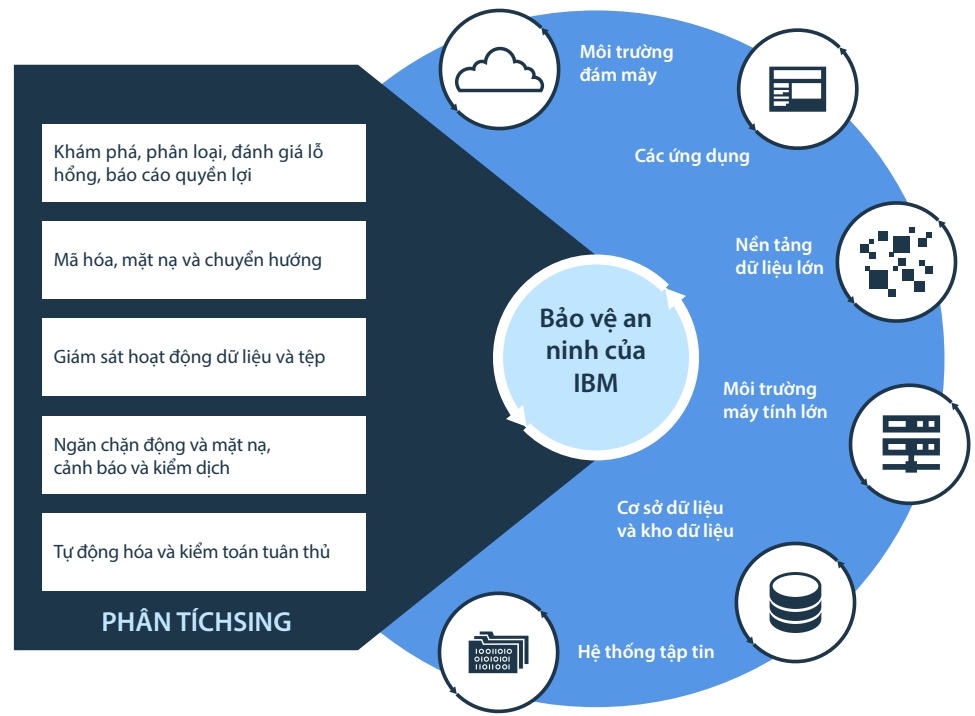
Guardium có thể giúp hỗ trợ chiến lược đám mây của bạn với các tính năng sau:

- Giám sát hoạt động của dữ liệu và tệp, đánh giá lỗ hổng, soạn dữ liệu, mã hóa dữ liệu, chặn, cách ly và cảnh báo theo cơ chế động
- Tự động phát hiện và phân loại dữ liệu nhạy cảm trên đám mây
- Che dấu dữ liệu tĩnh và động để đảm bảo mô hình truy cập ít đặc quyền nhất cho các tài nguyên đám mây
- Báo cáo kiểm toán và tuân thủ được xây dựng sẵn và tùy chỉnh theo các quy định khác nhau để chứng minh sự tuân thủ và tự động hóa quy trình tuân thủ trong môi trường tại cơ sở và đám mây.

5.2 Kết luận

Phần mềm Guardium mang tới giải pháp toàn diện cho các cơ sở hạ tầng vật lý, ảo và đám mây thông qua công cụ bảo mật tập trung, tự động trên nhiều môi trường đa dạng. Guardium giúp đơn giản hóa vấn đề tuân thủ, hạn chế rủi ro, cung cấp các hình ảnh sẵn sàng để cài đặt nhằm triển khai IaaS trên những nền tảng đám mây chính, chẳng hạn như IBM SoftLayer®, Microsoft Azure và Amazon Web Services, đồng thời vận hành trên các môi trường Microsoft Windows, UNIX và Linux.

Kiến trúc linh hoạt của Guardium cho phép thực hiện một số mô hình triển khai khác nhau. Bạn có thể chọn kiến trúc hệ thống phù hợp với doanh nghiệp mình: Tất cả cấu phần của Guardium có thể triển khai được trong đám mây hoặc bạn có thể chọn giữ lại tại cơ sở một vài trong các số cấu phần đó, chẳng hạn như trình quản lý trung tâm.



Hình 3: Guardium cung cấp giải pháp bảo vệ dữ liệu hoàn chỉnh trên nhiều môi trường và nền tảng công nghệ.

5.3 Kết luận

Sự linh hoạt này cho phép khách hàng hiện tại dễ dàng mở rộng chiến lược bảo vệ dữ liệu sang đám mây mà không ảnh hưởng tới các dự án triển khai hiện tại.

Các chương trình thu thập và giám sát dữ liệu đầu vào được triển khai trong đám mây có thể dễ dàng nạp dữ liệu vào trình quản lý trung tâm, đảm bảo bạn có được một góc nhìn tổng quan về các mối đe dọa trong vấn đề bảo vệ dữ liệu cho dù dữ liệu nằm ở đâu.

Các công cụ kiểm soát bảo mật cách ly tội phạm mạng ra khỏi kho dữ liệu - hoặc nhanh chóng phát hiện hành vi xâm nhập thành công - là những công cụ quan trọng. Nhưng trong kỷ nguyên của dữ liệu có tính di động, của các tải công việc thường xuyên thay đổi và công nghệ ảo hóa, việc giữ an toàn cho dữ liệu bằng cách mã hóa cũng không kém phần quan trọng.

Giải pháp bảo mật dữ liệu của IBM giúp bảo vệ dữ liệu nhạy cảm để các tổ chức có thể yên tâm rằng dữ liệu của họ được bảo vệ trong môi trường ảo và đám mây phức tạp.

5.4 Tài nguyên bổ sung

Giới thiệu về giải pháp của IBM Security

IBM Security cung cấp một trong các danh mục sản phẩm và dịch vụ bảo mật tích hợp và tiên tiến nhất dành cho doanh nghiệp. Danh mục này, do nhóm nghiên cứu và phát triển nổi tiếng thế giới IBM X-Force® hỗ trợ, cung cấp thông tin tình báo bảo mật để giúp các tổ chức bảo vệ toàn diện cho con người, cơ sở hạ tầng, dữ liệu và các ứng dụng, cũng như cung cấp các giải pháp quản lý danh tính và quyền truy cập, bảo mật cơ sở dữ liệu, phát triển ứng dụng, quản lý rủi ro, quản lý điểm cuối, bảo mật mạng, v.v..

Các giải pháp này cho phép tổ chức quản lý rủi ro một cách hiệu quả và triển khai chương trình bảo mật tích hợp cho thiết bị di động, đám mây, phương tiện truyền thông xã hội và các cấu trúc kinh doanh khác của doanh nghiệp. IBM vận hành một trong các tổ chức nghiên cứu, phát triển và cung cấp giải pháp bảo mật rộng lớn nhất trên thế giới, giám sát 15 tỉ sự kiện bảo mật mỗi ngày tại hơn 130 quốc gia và nắm giữ hơn 3.000 bằng sáng chế bảo mật.

Để biết thêm thông tin về vấn đề bảo mật dữ liệu, tuân thủ và đám mây, hãy truy cập **ibm.com**/guardium.

IBM Corporation
IBM Security
Route 100
Somers, NY 10589, Hoa Kỳ

Sản xuất tại Hợp chủng quốc Hoa Kỳ
Tháng 5 năm 2017

Tài liệu này được cập nhật đến ngày công bố lần đầu và có thể được IBM thay đổi bất cứ lúc nào. Không phải giải pháp nào cũng được cung cấp tại các quốc gia mà IBM hoạt động.

Khách hàng chịu trách nhiệm đảm bảo tuân thủ pháp luật và quy định áp dụng cho sản phẩm đó. IBM không đưa ra lời khuyên pháp lý, tuyên bố hay đảm bảo rằng dịch vụ hoặc sản phẩm của mình sẽ đảm bảo là khách hàng tuân thủ với bất kỳ điều luật hay quy định nào.

Tuyên bố thực hành bảo mật tốt nhất: Bảo mật hệ thống CNTT liên quan đến việc bảo vệ các hệ thống và thông tin thông qua phòng ngừa, phát hiện và phản ứng với hành vi truy cập trái phép từ bên trong và bên ngoài doanh nghiệp. Truy cập trái phép có thể dẫn đến thông tin bị thay đổi, phá hủy, chiếm dụng hoặc lạm dụng hoặc có thể dẫn đến thiệt hại hay lạm dụng các hệ thống của bạn, bao gồm cả để dùng trong các cuộc tấn công người khác. Không có hệ thống hay sản phẩm CNTT nào được coi là an toàn tuyệt đối và không có sản phẩm dịch vụ hay biện pháp bảo mật riêng lẻ nào có thể hiệu quả tuyệt đối trong việc ngăn chặn sử dụng hoặc truy cập trái phép. Các hệ thống, sản phẩm và dịch vụ của IBM được thiết kế như một phần của phương pháp bảo mật toàn diện, hợp pháp, nhất thiết có liên quan đến quy trình hoạt động bổ sung và có thể cần đến các hệ thống, sản phẩm hoặc dịch vụ khác để có hiệu quả cao nhất. IBM KHÔNG ĐẢM BẢO RẰNG MỌI HỆ THỐNG, SẢN PHẨM HOẶC DỊCH VỤ ĐỀU TRÁNH ĐƯỢC HÀNH VI GÂY HẠI HOẶC PHI PHÁP CỦA BẤT KỲ BÊN NÀO HOẶC SẼ GIÚP DOANH NGHIỆP CỦA BẠN TRÁNH ĐƯỢC ĐIỀU NÀY.

1. Thomas J. Bittman, "Đám mây riêng nội bộ không dành cho đa số doanh nghiệp thông thường," *Gartner*, ngày 22/5/2015.
2. Noel Yuhanna, "Ảo hóa dữ liệu doanh nghiệp, Quý 1 năm 2015," *The Forrester Wave*, ngày 11/03/2015.

Vui lòng tái chế

WGM12362-VNVI-00