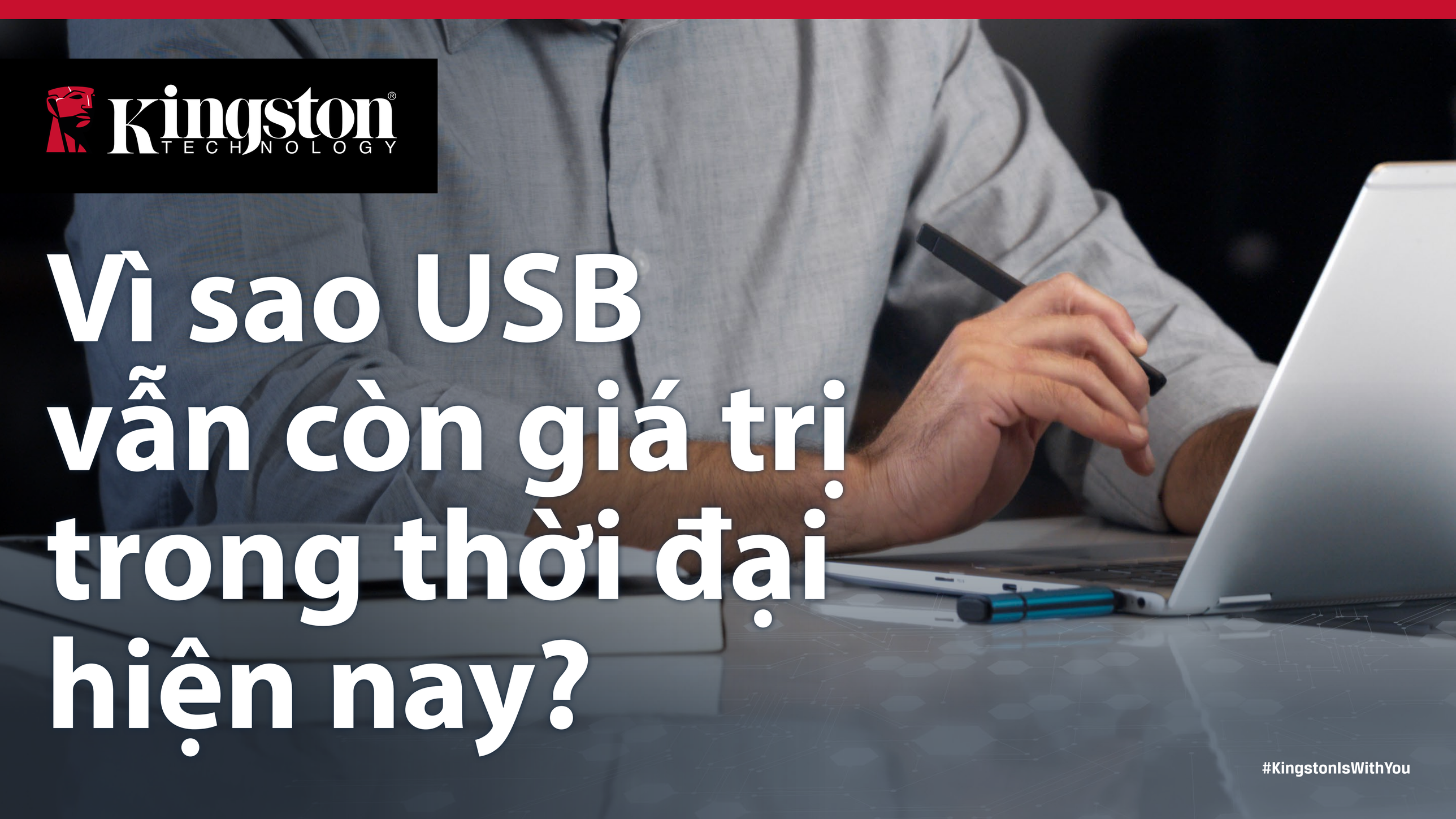

Kingston
TECHNOLOGY
Vì sao USB vẫn còn giá trị trong thời đại hiện nay?
#KingstonIsWithYou

Vì sao USB vẫn còn giá trị trong thời đại hiện nay?

Lời nói đầu và nội dung

Trong thời đại kỹ thuật số hiện nay, khi 60% dữ liệu doanh nghiệp trên toàn cầu được lưu trữ trên đám mây[1], có vẻ hơi kỳ quặc khi thảo luận về giá trị của một công nghệ lưu trữ đã sắp ba mươi năm tuổi. Tuy nhiên, kể từ khi ra mắt, phương tiện lưu trữ chính này vẫn đã và đang phát triển.

Đã qua lâu rồi cái thời USB chỉ là phương tiện tiêu chuẩn dùng để kết nối các tập tin, ổ đĩa và ứng dụng. Những giải pháp ngày nay không chỉ tự hào có được tốc độ truyền cải thiện hơn rất nhiều mà còn mang đến phương tiện bảo mật, dễ mang theo và đáng tin cậy không thể thiếu trong nhiều trường hợp. Nhưng giá trị của USB là gì trong khi các giải pháp lưu trữ trên đám mây dường như cũng có thể mang đến nhiều lợi ích tương tự?

Trong sách điện tử này, chúng tôi sẽ thảo luận về vị trí của ổ USB Flash giữa bối cảnh lưu trữ đám mây chiếm ưu thế. Dựa trên thông tin chuyên sâu từ một số chuyên gia đầu ngành, chúng tôi sẽ khám phá cách sử dụng USB của các tổ chức ngày nay và đàm luận về vị trí của USB giữa công nghệ mã hóa dựa trên phần mềm, môi trường lưu trữ độc lập và bảo mật dữ liệu điểm cuối.

Mục lục	Trang

Cộng tác viên

Cuốn sách điện tử này được ba chuyên gia trong ngành CNTT và các công nghệ mới nổi biên soạn.

Rafael Bloom

Rafael đã dành phần lớn sự nghiệp của mình hoạt động trong các vai trò cấp cao phụ trách về Sản phẩm công nghệ, Truyền thông tiếp thị và Phát triển kinh doanh. Hoạt động tư vấn của ông tập trung chủ yếu vào những thách thức mới về mặt tổ chức, sản phẩm và truyền thông khi có thay đổi về công nghệ và quy định. Trong vai trò vô cùng da dạng này, ông thể hiện chuyên môn của mình trong lĩnh vực quản trị thông tin và tuân thủ về mặt thiết kế, quyền riêng tư dữ liệu và các công nghệ mới nổi như AdTech, Mobile & 5G, AI và Học máy.

Tomasz Surdyk

Với hơn 24 năm kinh nghiệm trong lĩnh vực bảo mật CNTT trong các chính phủ, Tomasz là chuyên gia hàng đầu khi nói đến bảo mật thông tin, dữ liệu cá nhân và an ninh mạng. Trước đây, ông đã từng phụ trách kiểm tra các hệ thống và mạng ICT chuyên xử lý thông tin và dữ liệu cá nhân tối mật thuộc các cơ quan quản lý của chính phủ và có giấy phép an ninh ở NATO và EU. Trong vài năm qua, ông là chủ sở hữu của một công ty chuyên triển khai các giải pháp an ninh nhằm tăng cường bảo mật cho thông tin kinh doanh và dữ liệu cá nhân.

David Clarke

David được Thompson Reuter công nhận là một trong 10 người có tầm ảnh hưởng hàng đầu trong danh sách "Top 30 nhà lãnh đạo và nhà tư tưởng có ảnh hưởng nhất trên mạng xã hội về quản lý rủi ro, tuân thủ và công nghệ đăng ký tại Vương quốc Anh", đồng thời nằm trong danh sách 50 Chuyên gia toàn cầu hàng đầu của Kingston Technology. Trước kia, David từng đảm nhiệm nhiều vị trí quản lý bảo mật như Giám đốc toàn cầu về cung cấp dịch vụ bảo mật và Giám đốc cơ sở hạ tầng bảo mật cho các công ty FTSE 100 toàn cầu.

Sự lên ngôi của USB Flash

Khi USB (Universal Serial Bus) đầu tiên xuất hiện trên thị trường vào hơn 20 năm trước, khả năng tương thích đa dụng của sản phẩm này đã làm thay đổi cục diện của lĩnh vực công nghệ máy tính. Với khả năng hỗ trợ đông đảo người dùng dễ thực hiện nhiều thao tác trên thiết bị, chẳng mấy chốc USB đã phát triển mạnh mẽ. Nhất là ở đời USB Flash đầu tiên ra mắt vào năm 2000, tốc độ truyền dữ liệu đã nhanh hơn đáng kể, có cổng USB 3.0 và thậm chí là nhiều khả năng tuyệt vời khác.

Từ khi đó, công nghệ đã có một bước tiến dài về nhu cầu lưu trữ và bảo mật dữ liệu di động. Trọng tâm là thế hệ USB ngày nay – những ổ USB được thiết kế để sử dụng trong những trường hợp rất cụ thể. Đứng từ góc độ doanh nghiệp, mô hình làm việc từ xa và kết hợp ngày càng gia tăng, việc sử dụng dịch vụ đám mây và những mối quan ngại về an ninh mạng là những yếu tố đang thúc đẩy nhu cầu phải có những giải pháp hiệu quả hơn. Bên cạnh đó, các yêu cầu về mặt pháp lý đòi hỏi dữ liệu phải được lưu trữ theo cách tương thích. Những áp lực này thường nặng nề hơn nữa bởi vì các hệ thống phân tán và phức tạp có thể chạy "tại chỗ" và trên đám mây.

Tiếp đó là vấn đề gia tăng khối lượng dữ liệu có cấu trúc và phi cấu trúc, ví dụ như tài liệu, email, ảnh, video và siêu dữ liệu – mọi thứ đều khiến nhu cầu lưu trữ đang gia tăng của doanh nghiệp càng phức tạp thêm.

Nhưng nếu lưu trữ đám mây đã có thể giải quyết nhiều thách thức trong số này thì USB sẽ còn lại giá trị gì trong bối cảnh kinh doanh hiện tại?

> **"Khi nhắc đến USB, nhiều người sẽ nghĩ đến một phương tiện lỗi thời hoặc ít có giá trị vì không ít thì nhiều, trong quá khứ USB là thiết bị dùng một lần, có hiệu năng thấp và tính bảo mật thấp. - Rafael Bloom"**

Phương tiện lưu trữ dễ mang theo và đáp ứng được nhu cầu ngày càng gia tăng

Trong khi những kiểu sử dụng USB cũ hơn – tức là dùng làm một loại phương tiện lưu trữ dễ mang theo – đang dần biến mất thì ngày nay, xu hướng ngày một rõ nét là sử dụng USB hiệu năng cao để sao lưu cục bộ cá nhân, an toàn nhờ tăng cường lớp bảo vệ dữ liệu và bảo mật. Điều này có thể đóng vai trò vô cùng quan trọng đối với dữ liệu nhạy cảm về tuân thủ chẳng hạn như hồ sơ nhân sự, dữ liệu tài chính, hồ sơ y tế, bảo mật quyền sở hữu trí tuệ (IP) và tất cả các thông tin nhận dạng cá nhân (PII). Bên cạnh đó, thế hệ thiết bị này còn được cung cấp khả năng truyền dữ liệu, lưu trữ, sao lưu và bảo mật nhanh chóng, có thể sử dụng trong trường hợp:

- Thông tin pháp lý cần phải giao tận tay
- Tài liệu pháp lý và tài chính cần phải gửi và in tại chỗ hoặc bên ngoài
- Các môi trường bất lợi tiềm ẩn nơi mã độc tống tiền có thể trở thành một mối đe dọa
- Truyền dữ liệu đến hệ thống in không được phép truy cập mạng

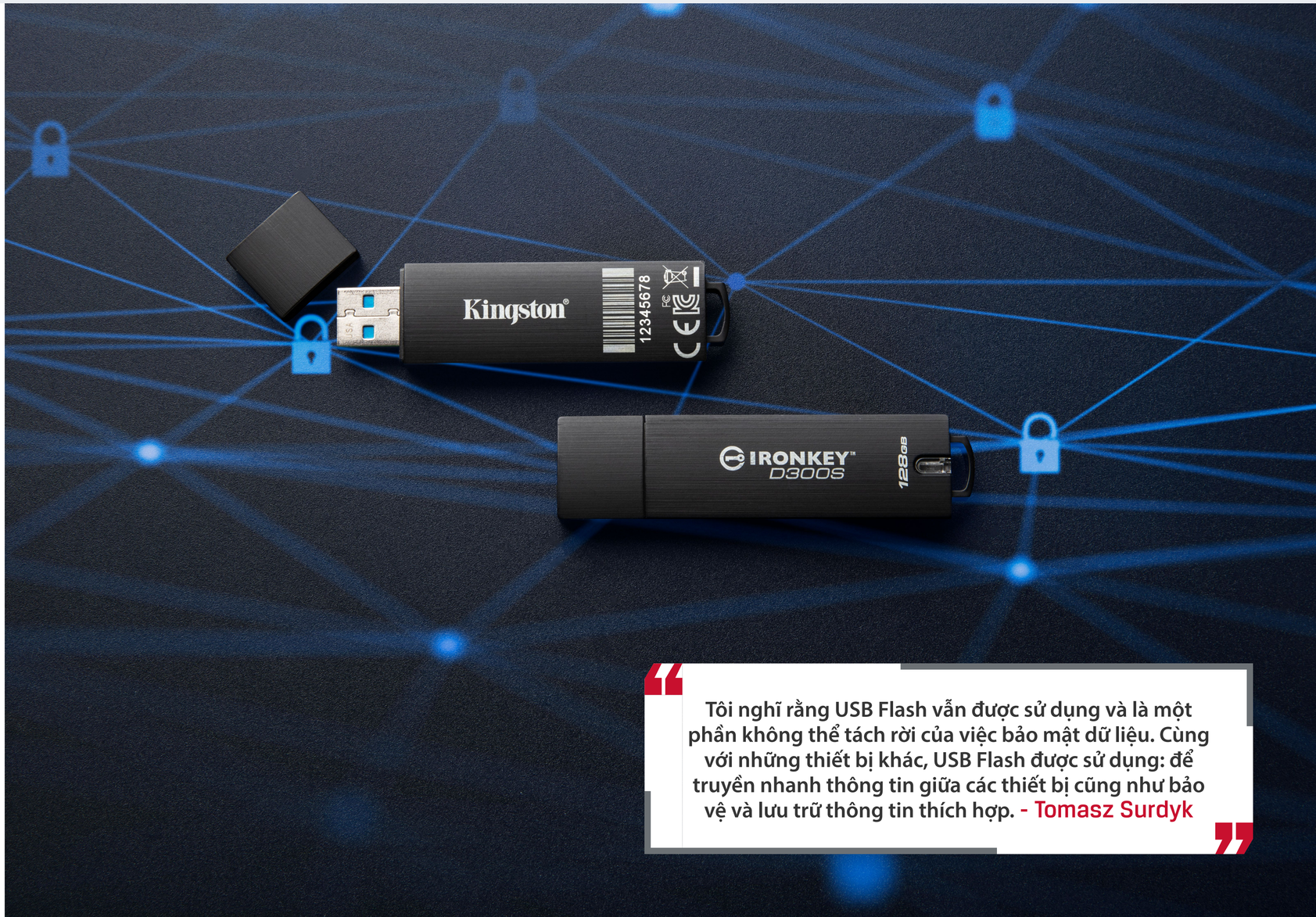
Nhà cung cấp USB mã hóa hàng đầu Kingston Technology đã bắt kịp với nhu cầu ngày càng tăng khi ra mắt các giải pháp chẳng hạn như Kingston IronKey™ S1000. Ổ USB mã hóa hàng đầu phân khúc này đã đáp ứng được các tiêu chuẩn nghiêm ngặt nhất với khả năng bảo vệ dữ liệu bảo mật khi cung cấp mã hóa XTS-AES 256 bit, cùng một con chip mã hóa riêng có khả năng bảo vệ chống can thiệp mạnh mẽ. Ngoài ra, ổ USB này còn được Chứng nhận FIPS 140-2 Cấp độ 3. Điều này đồng nghĩa với việc chính phủ Hoa Kỳ đã chính thức công nhận hiệu quả của ổ USB này dưới vai trò một phần cứng mã hóa, biến sản phẩm này thành phương tiện lý tưởng cho những tổ chức nào cần tăng cường đảm bảo bảo vệ dữ liệu.

Những ổ USB mã hóa phần cứng như thế mang đến các giải pháp quản lý thiết bị bảo mật tập trung, bất kể dữ liệu của họ lưu trữ trên nền tảng điện toán đám mây hay tại chỗ. Việc lưu trữ dữ liệu mã hóa tương thích theo cách dễ thực hiện mà không cần đến phần mềm cũng giúp đội ngũ CNTT tiết kiệm thời gian quý giá, mang đến các giải pháp được thiết kế để có thể triển khai nhanh chóng và hiệu quả.

Phương tiện lưu trữ dễ mang theo và đáp ứng được nhu cầu ngày càng gia tăng

Sao lưu và lưu trữ là một ví dụ khác khi người dùng có thể sử dụng USB để bảo vệ tài sản kỹ thuật số về lâu dài và độc lập với các dịch vụ Đám mây của bên thứ ba. Quả thật là người dùng có thể dễ dàng xử lý việc truyền dữ liệu lớn bằng Đám mây, nhưng IP độc quyền vẫn là dữ liệu nhạy cảm đáng được lưu trữ trên một ổ USB mã hóa, bảo mật, để được lưu trữ an toàn mà không dùng đến kết nối mạng.

Tiếp theo đó, sẽ luôn có những trường hợp khi tổ chức cần kiểm soát dữ liệu bằng lô-gíc và phần cứng, đặc biệt là khi sử dụng các ổ cứng mã hóa. Và cũng có những trường hợp lưu trữ trên ổ HDD/SSD không thể mã hóa được. Sử dụng ổ USB rời, được mã hóa, sẽ giúp bạn giải quyết vấn đề này, ví dụ như ổ Kingston IronKey D300S. Ổ USB Flash này có tính năng mã hóa phần cứng XTS Chuẩn mã hóa cao cấp 256-bit (AES), một loại mã hóa khối có thể mã hóa các khối dữ liệu 128 bit. Và khi có nhu cầu mã hóa dữ liệu hơn mức này, AES sẽ sử dụng chế độ mã hóa khối XTS có thể mang đến khả năng bảo vệ dữ liệu tốt hơn và mạnh mẽ hơn so với các chế độ trước đó.



> Tôi nghĩ rằng USB Flash vẫn được sử dụng và là một phần không thể tách rời của việc bảo mật dữ liệu. Cùng với những thiết bị khác, USB Flash được sử dụng: để truyền nhanh thông tin giữa các thiết bị cũng như bảo vệ và lưu trữ thông tin thích hợp. - Tomasz Surdyk

Mã hóa: So sánh mã hóa dựa trên phần cứng và mã hóa dựa trên phần mềm

Khi xem xét cách mã hóa dữ liệu, có thể lập luận rằng mã hóa phần cứng dễ quản lý hơn và an toàn hơn so với mã hóa phần mềm. Lý do là quá trình mã hóa được tách riêng với phần còn lại của hệ thống máy chủ, khiến kẻ gian khó lòng chặn hoặc xâm phạm vào thiết bị. Việc quản lý tập trung cấp thiết bị cho phép kiểm soát ổ qua mạng nội bộ LAN và Internet và có thể dùng làm một công cụ tuyệt vời để:

- Thiết lập và thực thi các chính sách sử dụng ổ USB mã hóa theo cá nhân và/hoặc nhóm
- Kiểm tra các hoạt động trên tập tin để theo dõi luồng dữ liệu ra vào tổ chức của bạn tốt hơn
- Cung cấp khả năng sao lưu nội dung từ xa cho việc vận chuyển dữ liệu quan trọng
- Vô hiệu hoá thiết bị từ xa khi ổ USB bị mất hoặc bị xâm nhập
- Tiến hành đặt lại mật khẩu từ xa khi quên mật khẩu

Khi các ổ được cấp phép đã được quản lý đúng theo cách này, nguy cơ bị sao chép và chia sẻ dữ liệu nhạy cảm sẽ được giảm thiểu. Ngoài ra, USB mã hóa phần cứng thời nay cũng mang đến rất nhiều tính năng bảo mật bổ sung, giúp ngăn người khác truy cập và đọc các tập tin hoặc tin nhắn trái phép, trừ người nhận dự kiến.

> **Tôi tin rằng mã hóa phần cứng tốt hơn mã hóa phần mềm. Điểm khác biệt quan trọng giữa hai phương pháp mã hóa phần cứng và phần mềm là khả năng dễ bị tấn công bằng phương pháp bruce force. Trong trường hợp thiết bị mã hóa ổ cứng, chống lại những cuộc tấn công như thế là điều không hề khó khăn.**
>
> - Tomasz Surdyk

Mã hóa: So sánh mã hóa dựa trên phần cứng và mã hóa dựa trên phần mềm

Dù các doanh nghiệp có thể cân nhắc sử dụng mã hóa phần mềm vì lý do chi phí nhưng nước đi này có thể sẽ hơi thiển cận. Các giải pháp dựa trên phần mềm sử dụng chung tài nguyên mã hóa của thiết bị chủ với các chương trình khác, vì thế dữ liệu chỉ được an toàn khi máy tính vẫn an toàn và thường xuyên cần phải cập nhật phần mềm – nếu không cập nhật liên tục, bạn sẽ dễ bị tấn công. USB mã hóa phần mềm có thể bị đoán mật khẩu khi bị tấn công không giới hạn bằng phương pháp brute force và cũng không có biện pháp chống lại phương pháp tấn công dictionary attack – phương pháp này có thể kiểm tra hàng triệu tổ hợp ký tự chỉ trong một khoảng thời gian ngắn.

Bên cạnh đó, mã hóa phần mềm cũng là loại mã hóa có thể xoá bỏ được. Bất cứ nhân viên nào giữ ổ cứng mã hóa phần mềm cũng có thể sao chép dữ liệu, định dạng USB và như thế là mã hóa đã bị xoá. Sau đó, họ có thể sao chép lại tập tin dữ liệu và sử dụng ổ cứng mà không cần phải xác thực rắc rối trên những nền tảng và hệ điều hành khác.

Như chúng tôi đã đề cập trước đó, với việc mã hóa dựa trên phần cứng, "mã hóa" phần cứng – và việc lưu trữ dữ liệu sau đó – sẽ diễn ra độc lập với hệ thống máy chủ. Điều này đảm bảo rằng sẽ có một bức tường phòng thủ bổ sung khi hệ thống bị xâm nhập.

Không thể xem nhẹ điều này, đặc biệt là đối với các ngành như tài chính, y tế và chính phủ. Lý do là vì những quy định chẳng hạn như Đạo Luật về Trách nhiệm giải trình và Cung cấp thông tin bảo hiểm y tế (HIPAA) và Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS) thường có những yêu cầu nghiêm ngặt về việc mã hóa thông tin nhạy cảm.

Việc sử dụng thiết bị mã hóa phần cứng mạnh mẽ để tuân thủ những quy định này sẽ giúp các tổ chức tránh được khoản tiền phạt, kiện tụng đắt đỏ và thiệt hại nghiêm trọng về danh tiếng có thể xảy ra. Dù ổ cứng mã hóa phần cứng có thể tốn kém hơn so với USB thương mại giá rẻ, nhưng chi phí pháp lý của một vụ vi phạm – tính đơn giản như tiền phí vài giờ tư vấn pháp lý – là đủ để bạn có thể dễ dàng mua được hàng trăm ổ cứng.

Nhu cầu bảo vệ dữ liệu nhạy cảm ngày càng gia tăng

> Mã hóa mọi dữ liệu nhanh nhất có thể, sao lưu bằng Phương pháp 321 (có thể chọn USB vì đã có sẵn) và thực hiện khả năng phân đoạn vi mô nhanh chóng.
> - David Clarke

Khi nói đến việc bảo vệ dữ liệu nhạy cảm không bị thất thoát và mất cắp, mỗi tổ chức đều có nghĩa vụ đảm bảo các thiết bị của họ đã có đầy đủ những tính năng bảo mật. Điều quan trọng nữa cần lưu ý là cho dù có vô số các mối đe dọa trên không gian mạng – với mức độ không ngừng gia tăng – nhưng độ trưởng thành kỹ thuật số và kỹ năng quản lý dữ liệu điểm cuối của chính người dùng vẫn là một yếu tố rủi ro đáng chú ý nếu không được xử lý. Mối đe dọa nội bộ bao gồm mất kiểm soát dữ liệu hoặc thiết bị lưu trữ USB, truyền dữ liệu ở môi trường không an toàn, sử dụng USB không mã hóa và dùng chung mật khẩu đều có thể là kết quả của việc rà soát, suy xét chưa đủ sát sao từ phía người dùng cuối. Tất cả những rủi ro đó đều có thể tránh được bằng cách đào tạo, trang bị kiến thức đầy đủ và sử dụng giải pháp USB phù hợp.

> Tổ chức nên có một bản đồ dữ liệu rõ ràng, bao gồm mức độ quan trọng và/hoặc nhạy cảm của mọi bộ dữ liệu, kèm theo kế hoạch ưu tiên xử lý các dữ liệu quan trọng nhất bằng cách ngắt kết nối thiết bị với dữ liệu, hoặc tắt cổng truyền của nguồn dữ liệu. Điều quan trọng nhất là có thể nhanh chóng cô lập các hệ thống bị ảnh hưởng – và một lần nữa, có sẵn một kế hoạch rõ ràng trên hồ sơ và đã thực hành là điều tối cần thiết.
> - Rafael Bloom

Việc lập kế hoạch trước và có được một cấu trúc thông tin liên lạc đã được luyện tập nhuần nhuyễn cũng là yếu tố then chốt để giải quyết một mối đe dọa sống còn có thể xảy ra. Những mối đe dọa trên không gian mạng ngày nay đều nhắm đến điểm yếu của các tổ chức.

Thời điểm tốt nhất để soạn ra kế hoạch sử dụng USB mã hóa là trước khi thật sự cần đến kế hoạch đó, bằng cách đưa USB mã hóa và các chính sách vào chiến lược bảo mật tổng thể của tổ chức. Khi không có sẵn kế hoạch sử dụng USB mã hóa và không có hướng dẫn, bạn sẽ không có cơ sở để phát triển thêm và tổ chức của bạn sẽ có nguy cơ gặp rủi ro ở mọi cấp độ – bao gồm việc không tuân thủ quy định, chẳng hạn như Quy định chung về bảo vệ dữ liệu (GDPR) có điều 32 nêu rõ rằng dữ liệu nhạy cảm phải được mã hóa.

> Dữ liệu nhạy cảm do người dùng xử lý. Đánh mất dữ liệu sẽ làm tăng trách nhiệm và ảnh hưởng đáng kể đến hình ảnh và sự an toàn của công ty. Nên sử dụng nhiều giải pháp bảo mật để bảo vệ dữ liệu nhạy cảm, bao gồm cả việc mã hóa dữ liệu. - Tomasz Surdyk

Bảo mật dữ liệu tài chính nhạy cảm

Ngoài những tác động bảo mật, các giải pháp lưu trữ và sao lưu dữ liệu cũng phải tuân theo những tiêu chuẩn tuân thủ. Một vài quy tắc trong số đó rất phổ biến trong những ngành dọc, chẳng hạn như nhu cầu quản lý và áp dụng kế hoạch lưu trữ dữ liệu, trong khi những quy tắc khác được xử lý rất khác biệt, chẳng hạn như việc di chuyển dữ liệu doanh nghiệp lên đám mây.

Trong nhiều ngành dọc, chẳng hạn như dịch vụ tài chính, các quy định đã có hiệu lực và bắt buộc các đơn vị phải quản lý dữ liệu đúng cách. Nhất là ngân hàng, ngành rất kín tiếng trong việc sử dụng bên thứ ba để lưu trữ và sao lưu vào lúc ban đầu, và nhiều ngân hàng vẫn khăng khăng sở hữu mọi cơ sở hạ tầng dữ liệu của họ.

Các tổ chức tài chính cũng phải tuân thủ theo danh sách quy định và tiêu chuẩn bảo mật dữ liệu đang ngày một tăng dần, ví dụ như Đạo luật Sarbanes-Oxley (SOX) và Quy định chung về bảo vệ dữ liệu (GDPR). Tuy nhiên, khi số lượng nhân viên hợp đồng và nhân viên lưu động ngày một tăng, nguy cơ rò rỉ dữ liệu và việc không tuân thủ các quy định do các luật và tiêu chuẩn đó đặt ra cũng tăng theo.

Sự thật là những việc cố gắng tuân thủ theo quy định có thể dễ dàng bị ảnh hưởng nếu nhân viên lưu động không thể bảo vệ danh tính kỹ thuật số của mình, không gian làm việc di động, hồ sơ khách hàng và dữ liệu tài chính mà họ mang theo. Đó là lý do mà ngày càng nhiều tổ chức đang chuyển sang sử dụng những giải pháp bảo mật di động như USB mã hóa Kingston IronKey để bảo vệ danh tính và ứng dụng kỹ thuật số, bất kể nhân viên mang thiết bị đến đâu.

> **“Khi xem xét xu hướng tổng thể là chuyển sang không gian CNTT phân tán hơn và khả năng thay đổi quy mô của cơ sở hạ tầng Đám mây, rất dễ dàng nhận thấy phần lớn các ngành và hàng loạt những doanh nghiệp vừa và nhỏ đã không còn quan ngại về việc quản lý các phòng máy chủ đông lạnh. - Rafael Bloom”**

Truy cập bảo mật vào dữ liệu sức khoẻ bệnh nhân

Y tế cũng là một ngành đề cao bảo mật dữ liệu hơn bao giờ hết. Thậm chí thông tin bệnh nhân còn phải đối mặt với nguy cơ mất cắp lớn hơn, với các vụ vi phạm đã làm lộ hồ sơ của tổng cộng 45,67 triệu bệnh nhân trong năm 2021 – con số hàng năm lớn nhất kể từ năm 2015[2]. Khi bàn về việc lưu trữ và sao lưu dữ liệu, dữ liệu của bệnh nhân là thông tin y tế rất quan trọng và toàn diện, giúp nhà cung cấp dịch vụ y tế có thể điều trị cho bệnh nhân an toàn.

Dữ liệu này có thể bao gồm tất cả thông tin từ tập tin Hồ sơ sức khoẻ điện tử (EHR) chứa bệnh sử, các xét nghiệm, ảnh chụp và ảnh chụp X quang, cho đến các tập tin quản trị chứa hồ sơ bảng lương, bảo hiểm của bệnh nhân và các khoản phải trả. Đối diện với lực lượng lao động di động ngày một đông và thị trường y tế toàn cầu đang trải qua những biến động và biến đổi to lớn, không khó để hiểu vì sao những nhà cung cấp dịch vụ y tế ngày nay lại quan tâm đến việc bảo mật dữ liệu đến vậy.

> **Trước thực trạng mã độc tống tiền ngày nay đáng báo động đến mức phát triển như một "ngành" riêng, mỗi tổ chức xử lý dữ liệu bảo mật đều cần phải cân nhắc cách thức hoạt động giữa bối cảnh luôn phải cẩn trọng này. - Rafael Bloom**

Thêm vào đó, nếu không thể dự đoán trước rủi ro và tuân thủ theo những quy định nghiêm ngặt như Đạo Luật về Trách nhiệm giải trình và Cung cấp thông tin bảo hiểm y tế (HIPAA) hoặc Đạo luật công nghệ thông tin y tế cho y tế kinh tế và lâm sàng (HITECH) thì tình trạng vi phạm dữ liệu y tế gây tốn kém sẽ diễn ra và xa hơn nữa là làm lung lay lòng tin của bệnh nhân, đối tác hoặc cơ quan quản lý.

Với những giải pháp chẳng hạn như dòng USB mã hóa của Kingston IronKey, các tổ chức y tế có thể thiết lập chính sách mật khẩu, sử dụng ứng dụng, phục hồi và nhiều hơn nữa – trên một số ít hoặc hàng nghìn USB chỉ từ một bảng điều khiển duy nhất. Những nhân viên lưu động và nhân làm việc trực tiếp với bệnh nhân sẽ có thể hỗ trợ được nhiều người hơn nhờ vào những giải pháp dễ sử dụng mà không cần phải cài đặt trình điều khiển hoặc phần mềm khác để truy cập an toàn vào kho dữ liệu lưu trữ. Người dùng và quản trị viên có thể hạn chế phạm vi dữ liệu dễ dàng và nhanh chóng dù dữ liệu đã được truyền đến nơi nào.

Vị trí của USB khi lưu trữ đám mây chiếm ưu thế trong tương lai

> **Lưu trữ dữ liệu trên đám mây là hiện tại và tương lai. Tôi vẫn lập luận rằng bảo mật thông tin bằng phần cứng, VD: sử dụng USB mã hóa, là biện pháp an toàn nhất. Người dùng không thể toàn quyền kiểm soát những gì diễn ra trong đám mây. Tuy nhiên, chúng ta có thể kiểm soát dữ liệu trong USB mã hóa mà chúng ta tự bảo mật và lưu trữ. Trừ chúng ta ra thì sẽ không ai có thể truy cập vào những phương tiện đó nữa.**
> - Tomasz Surdyk

Giờ đây khi đã thấy rõ những ưu điểm của USB, vậy chính xác thì vai trò của USB là gì khi lưu trữ đám mây chiếm ưu thế trong tương lai?

Vào một thập kỷ trước, người ta có nhu cầu sử dụng USB rất lớn vì đó là công cụ chính để lưu trữ và truyền dữ liệu thuận tiện. Tuy nhiên, dưới tác động của mô hình làm việc kết hợp và những đội ngũ phân tán, giờ đây đám mây có thể giúp truy cập thông tin đã lưu trữ nhanh chóng và đơn giản từ nhiều thiết bị khác nhau. Dù ổ flash đã từng vô cùng phổ biến nhờ vào tính thoải mái độc đáo mà dòng sản phẩm này đem lại khi truyền tập tin. Ngày nay, dịch vụ lưu trữ đám mây đã mang đến khả năng di chuyển tập tin dễ dàng hơn.

Dù thế, lưu trữ đám mây vẫn còn rất nhiều hạn chế. Lưu trữ đám mây cần phải có kết nối mạng – không chỉ ảnh hưởng đến cách thức và thời gian sao lưu hoặc truyền tập tin mà còn tăng thêm mối quan ngại về tính bảo mật. Khi một công ty đưa ra quy định sử dụng đám mây, không nhất thiết công ty đó phải kiểm soát được nơi truy cập vào dữ liệu. Vì thế, chỉ với một thao tác đơn giản là truy cập vào VPN bằng kết nối Wifi công cộng hoặc cá nhân, người dùng đã tạo ra nguy cơ bị xâm nhập. Ngoài ra, dịch vụ Đám mây còn rất hấp dẫn đối với những tác nhân độc hại, khi phần lớn mọi phần mềm độc hại (61%) đều được phân phối qua các ứng dụng đám mây[3].

> **Có lẽ điều nên làm là xem xét tình huống gì sẽ xảy ra khi đám mây không khả dụng, những tình huống yêu cầu dữ liệu luôn phải có sẵn 100% và trường hợp lưu trữ thông tin lâu dài có thể tạo ra lỗ hổng.**
> - David Clarke

Vị trí của USB khi lưu trữ đám mây chiếm ưu thế trong tương lai

Mặt khác, người dùng có thể mã hóa USB bằng phần cứng của thiết bị hoặc thông qua phần mềm. Mã hóa tập trung vào phần cứng, không dùng phần mềm là cách hữu hiệu nhất để bảo vệ trước các cuộc tấn công mạng. Đó là một giải pháp tuyệt vời và đơn giản để chống vi phạm dữ liệu và có thể đáp ứng được những tiêu chuẩn tuân thủ nghiêm ngặt với tính bảo mật tân tiến nhất trong bảo vệ dữ liệu để giúp các tổ chức tự tin quản lý nguy cơ và giảm rủi ro.

Vì những thiết bị này hoạt động độc lập, USB mã hóa phần cứng không cần phần mềm trên máy tính chủ. Do không có lỗ hổng phần mềm nên cũng loại bỏ khả năng bị tấn công bằng phương pháp brute force, sniffing và băm bộ nhớ. USB mã hóa phần mềm còn phải đối mặt với rủi ro là bất cứ người dùng nào cũng có thể vô hiệu hoá mã hóa bằng cách định dạng lại ổ cứng trên bất kỳ máy tính nào và sử dụng ổ cứng để lưu trữ dữ liệu nhạy cảm theo cách không được bảo vệ.

USB mã hóa phần cứng cũng mang đến một phương tiện phần cứng đặc biệt để bảo mật dữ liệu. Chúng cho phép người dùng hoặc quản trị viên thiết lập tiêu chí truy cập thông tin và có thể tích hợp với giải pháp điểm cuối cục bộ đã có trước đó. Do đó, USB mã hóa là một giải pháp thuận tiện và tiết kiệm chi phí trong nhiều tình huống khi lưu trữ đám mây không hoạt động hoặc không phải là giải pháp hiệu quả. Tình huống đó có thể là khi cần lưu trữ dữ liệu từ một thiết bị không kết nối mạng, cần phải ở chế độ riêng tư hoặc cần có quyền truy cập khi đang ngoại tuyến.

> **Nếu chúng ta chia dữ liệu thành dữ liệu 'nóng' hoặc 'lạnh' dựa trên mức độ hữu ích hàng ngày đối với một tổ chức thì có lẽ, đặt dữ liệu 'lạnh' vào đám mây và lưu trữ cục bộ dữ liệu 'nóng' trên USB sẽ mang đến hiệu quả cao hơn nếu tính liên tục trong hoạt động và hiệu năng cao là điểm cần ưu tiên của tổ chức, phòng ban hoặc một quy trình quan trọng cụ thể của doanh nghiệp. - Rafael Bloom**

Tóm tắt

Dù chúng tôi không thể dự đoán được trong tương lai sẽ xuất hiện thêm những đổi mới nào, nhưng điều chúng tôi có thể mang đến là một danh mục USB đã đạt giải thưởng, cung cấp một loạt các giải pháp mã hóa năng động dành cho mọi cấp độ yêu cầu bảo vệ dữ liệu di động. Từ USB được trang bị bàn phím chữ và số để bảo vệ mã PIN và dễ dàng sử dụng; cho đến chứng nhận FIPS 140-2 Cấp độ 3 để có cấp độ mã hóa cao nhất cùng với khả năng bảo vệ chống can thiệp; và công nghệ USB SuperSpeed 3.1 không làm ảnh hưởng đến tính bảo mật, các sản phẩm của Kingston IronKey được thiết kế để giải quyết những thách thức về dữ liệu của bạn với ổ USB hứa hẹn mang đến giải pháp vận chuyển dữ liệu và lưu trữ dữ liệu di động hiệu quả và mạnh mẽ.

Đội ngũ chuyên môn với các chuyên gia của chúng tôi luôn sẵn sàng hỗ trợ từng bước trên hành trình bảo vệ dữ liệu của bạn, là người hỗ trợ đáng tin cậy giúp bạn tìm được giải pháp lưu trữ phù hợp với nhu cầu của bạn.

Chúng tôi có kỹ năng và khả năng kỹ thuật để giúp giữ các thông tin bảo mật được an toàn và tuân thủ theo quy định mới, dù bạn đang muốn soạn kế hoạch sử dụng USB mã hóa, xác định loại USB tốt nhất cho doanh nghiệp của mình hay thiết lập và thực thi các chính sách bảo mật. Chúng tôi cung cấp dịch vụ có tính cá nhân hóa cao và cam kết đem lại những sản phẩm có khả năng hỗ trợ những ưu tiên lưu trữ dữ liệu của bạn, cho phép bạn bắt kịp tốc độ di chuyển chưa từng thấy của thế giới kinh doanh.

Giới thiệu về Kingston

Với 35 năm kinh nghiệm, Kingston có kiến thức để xác định và giải quyết các thách thức về dữ liệu di động – giúp lực lượng lao động của bạn có thể dễ dàng làm việc một cách an toàn mà không làm tổn hại đến tổ chức.

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers

#KingstonIsWithYou