



Giải thích và khám phá Giải pháp bảo mật thiết bị đầu cuối tối ưu được hợp tác sản xuất với Matrix42

MATRIX42

#KingstonIsWithYou

Giải thích và khám phá Giải pháp bảo mật thiết bị đầu cuối tối ưu được hợp tác sản xuất với Matrix42

Giới thiệu

Trong thế giới ngày nay, bảo vệ dữ liệu là một yêu cầu cơ bản của các doanh nghiệp, chính phủ và cá nhân.

Vi phạm dữ liệu, xâm nhập và những sự cố do con người gây ra là những lời nhắc nhở thường xuyên về các mối đe dọa và nguy cơ trên khắp toàn cầu. Các chi phí tài chính và phí tổn danh tiếng liên quan đến một vụ xâm phạm dữ liệu có thể vô cùng lớn. Tất cả các yêu cầu về an ninh mạng nâng cao và chiến lược chống thất thoát dữ liệu (DLP) trên thiết bị đầu cuối đều phụ thuộc vào bộ nhớ và thiết bị lưu trữ hiệu quả, tin cậy.

Việc sử dụng công nghệ mã hóa, bộ nhớ và thiết bị lưu trữ nhanh kết hợp với các tiêu chuẩn, chính sách và các quy tắc thực hành tốt nhất là một bước tiến lớn. Máy tính xách tay và USB bị thất lạc khiến cho các cá nhân và công ty đều dễ bị tổn thương trước sự cố làm lộ thông tin cá nhân và riêng tư. Kingston cung cấp các giải pháp ngăn ngừa mối đe dọa để giúp giảm thiểu nguy cơ, đồng thời bổ sung cho một kế hoạch bảo mật hiện có hoặc đang được phát triển.



Nội dung

Cuốn sách điện tử ngắn gọn này sẽ trình bày về các giải pháp thiết bị đầu cuối và những trường hợp mà USB mã hóa cùng chương trình tùy chỉnh của Kingston, kết hợp với phần mềm bảo vệ dữ liệu EgoSecure của Matrix42 đã hỗ trợ giải quyết các thách thức trong sáu lĩnh vực khác nhau, đồng thời đưa ra giải pháp phù hợp với nhu cầu của doanh nghiệp họ.

Chúng ta sẽ tìm hiểu sâu hơn về sáu lĩnh vực này và xem cách họ xử lý những thách thức bảo mật thiết bị đầu cuối trong doanh nghiệp của mình.

Mục lục

Phần 1	Tình huống điển hình trong ngành – Lĩnh vực công	4
Phần 2	Tình huống điển hình trong ngành – Chăm sóc sức khỏe	5
Phần 3	Tình huống điển hình trong ngành – Tài chính	6
Phần 4	Tình huống điển hình trong ngành – Ô tô	7
Phần 5	Tình huống điển hình trong ngành – Viễn thông	8
Phần 6	Tình huống điển hình trong ngành – Sản xuất	9
Phần 7	Các giải pháp của Kingston và Matrix42	10
	Tóm tắt	11
	Giới thiệu về Kingston	12



Phần 1: Tình huống điển hình trong ngành Lĩnh vực công



Tình huống:

Việc sử dụng các thiết bị USB rất phổ biến trong lĩnh vực công. Ví dụ: các văn phòng đảm bảo trật tự công cộng phải sao chép ảnh được chụp về những người vi phạm quy định đậu xe hoặc vi phạm quy định hành chính từ máy ảnh kỹ thuật số sang hệ thống của cơ quan chức năng thông qua dây cáp USB. Cơ quan công an nhận dữ liệu điều tra trên thiết bị lưu trữ dữ liệu bên ngoài. Cần phải ghi lại dữ liệu này và ngăn truy cập trái phép.

Thách thức:

Do nhu cầu sử dụng USB cao nên các nhân viên thường xuyên yêu cầu được cung cấp USB. Cần ngăn chặn việc sử dụng các thiết bị lưu trữ dữ liệu riêng tư và trái phép vì lý do bảo mật. Nếu một nhân viên cần thiết bị lưu trữ USB mới, thì phải cung cấp thiết bị lưu trữ này nhanh nhất có thể thông qua Bộ phận trợ giúp người dùng để không ảnh hưởng đến công việc của nhân viên đó. Điều quan trọng là cần lưu ý rằng sẽ không phát sinh bất kỳ sự cố bảo mật nào nếu sử dụng thiết bị USB phù hợp.

Giải pháp:

Bằng cách kết hợp các công nghệ điều khiển thiết bị, lọc dữ liệu và mã hóa, có thể thực hiện kịch bản sau đây:

Các thiết bị không xác định thường bị chặn trên thiết bị đầu cuối của máy tính. Các thiết bị lưu trữ dữ liệu như máy ảnh kỹ thuật số chỉ được phép sử dụng cho một số chức năng nhất định như đọc tệp hình ảnh. Các thao tác ghi thường được mã hóa và chỉ được phép thực hiện trên các thiết bị USB được cho phép. Tất cả các hoạt động truy cập dữ liệu đều được ghi nhật ký. Có thể đơn giản hóa hoạt động quản lý các thiết bị được cho phép bằng cách tùy chỉnh số sê-ri và ID phần cứng. Do đó, ứng dụng Quản lý dịch vụ Matrix42 cho phép người dùng yêu cầu USB Kingston Technology được cá nhân hóa trên Cổng thông tin tự phục vụ. Sau khi quy trình phê duyệt hoàn thành, thiết bị USB sẽ được tự động cho phép sử dụng trong phần mềm bảo vệ dữ liệu EgoSecure.

“ Các nhân viên của chúng tôi rất hào hứng vì thiết bị USB được cung cấp một cách dễ dàng và nhanh chóng sau khi thực hiện quy trình phê duyệt ngắn gọn. Chúng tôi rất hài lòng với chương trình tùy chỉnh của Kingston Technology và khả năng quản lý dễ dàng nhờ sự kết hợp giữa quản lý dịch vụ và bảo mật thiết bị đầu cuối của Matrix42. ”

Trưởng bộ phận Trợ giúp, Lĩnh vực công



Phần 2: Tình huống điển hình trong ngành Chăm sóc sức khỏe

Tình huống:

Các thiết bị lưu trữ bên ngoài vẫn thường xuyên được dùng làm phương tiện trao đổi dữ liệu với nhân viên và các tổ chức khác.

Ví dụ: các bệnh viện tại Đức phải cung cấp cho hệ thống Ghi nhận ung thư thông tin về các ca ung thư hiện tại và tiến triển của họ. Để dễ dàng thực hiện, dữ liệu thường được chuyển thông qua các thiết bị lưu trữ dữ liệu di động.

Các bác sĩ cũng thích tích hợp tài liệu, chẳng hạn như dữ liệu nghiên cứu, vào bài giảng của họ thông qua USB.

Thách thức:

Dữ liệu bệnh nhân vô cùng nhạy cảm và không được để chúng rơi vào tay những người không được phép. Do đó, cần tăng cường và củng cố hơn nữa hoạt động bảo vệ dữ liệu. Việc thất lạc thiết bị truyền dữ liệu có thể trở thành một vấn đề lớn, vì điều này không những vi phạm quy định GDPR mà còn ảnh hưởng đến sức khỏe của bệnh nhân. Do đó, cần kiểm soát, giám sát và mã hóa việc truy cập vào bộ lưu trữ dữ liệu USB.

Giải pháp:

Phần mềm bảo vệ dữ liệu EgoSecure kết hợp nhiều biện pháp bảo vệ khác nhau, như kiểm soát truy cập, kiểm tra dữ liệu, lọc và mã hóa trong một giải pháp duy nhất. Các quản trị viên CNTT được trao quyền quyết định những nhân viên nào được cấp quyền truy cập và các thiết bị được phép truy cập. Có thể cho phép trường hợp ngoại lệ, ví dụ: theo số sê-ri và ID phần cứng. Có thể xác định các mã số định danh này nhờ chương trình tùy chỉnh của Kingston Technology, sao cho chỉ một giá trị duy nhất cần được cấu hình trong việc quản lý phần mềm bảo vệ dữ liệu EgoSecure để chỉ cho phép sử dụng các thiết bị đã được công ty phê duyệt. Điều này giúp giảm thiểu đáng kể nỗ lực quản trị và tăng cường bảo mật dữ liệu (GDPR, CCPA, HIPAA, v.v.), vì quyền truy cập được mã hóa và giám sát.

“Chúng tôi hiện đã sử dụng USB được mã hóa của Kingston. Giờ đây, với phần mềm Bảo vệ dữ liệu EgoSecure, chúng tôi còn có thể đảm bảo hiện thực hóa khả năng truy xuất nguồn gốc của hoạt động chuyển dữ liệu bệnh nhân, tuân theo quy định GDPR của EU.”

**Giám đốc bảo mật thông tin,
Bệnh viện Đại học**



Phần 3: Tình huống điển hình trong ngành Tài chính



Tình huống:

Ngân hàng phải đáp ứng nhiều yêu cầu tuân thủ khác nhau. Một trong những yêu cầu đó là tuân thủ PCI-DSS (Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán). Các yêu cầu PCI-DSS bao gồm nhu cầu mã hóa dữ liệu, phân tích lỗ hổng bảo mật và lọc dữ liệu. Mục tiêu là hạn chế tối đa hoặc ngăn chặn hoàn toàn các mối đe dọa và nguy cơ bảo mật CNTT.

Thách thức:

Có rất nhiều nguy cơ về bảo mật CNTT đang tồn tại trên thiết bị đầu cuối. Hàng ngày, nhân viên phải làm việc với thông tin thẻ thanh toán từ người tiêu dùng và doanh nghiệp, đồng thời xử lý dữ liệu nhạy cảm từ các tổ chức tài chính. Do đó, họ phải đối mặt với mối đe dọa rằng dữ liệu từ đám mây, email, USB và trang web có thể bị phần mềm độc hại xâm phạm hoặc dữ liệu đó có thể vô tình rơi vào tay các bên thứ ba nếu không được bảo vệ đầy đủ. Sự cố như vậy sẽ là một mối nguy cơ, tiềm ẩn những tác động tài chính tới ngân hàng vì họ đã vi phạm các quy định GDPR, PCI-DSS và đạo luật Sarbanes-oxley. Hơn nữa, tội phạm mạng đang cố gắng gây ảnh hưởng hoặc thao túng các hệ thống ngân hàng bằng nhiều cách thức khác nhau và ngày càng tinh vi hơn. Ví dụ: gần đây đã xảy ra một vụ tội phạm mạng liên quan đến các máy ATM bị gián đoạn nguồn cấp điện. Do đó, tội phạm đã khởi động hệ thống bằng thiết bị USB có thể boot nhằm đánh cắp tiền.

Giải pháp:

Cần bảo mật các hệ thống CNTT bằng những biện pháp bảo vệ nhiều lớp. Có thể thực hiện điều này thông qua các công nghệ kiểm soát ứng dụng, kiểm soát thiết bị, phát hiện bất thường, UEBA (Phân tích hành vi của người dùng và thực thể), giám sát và mã hóa toàn bộ ổ đĩa bằng tính năng Xác thực trước khi khởi động. Matrix42 có thể triển khai giải pháp này trong một hệ sinh thái tự động và tích hợp để chỉ cho phép các ứng dụng và thiết bị USB mã hóa được cho phép. Ngoài ra, hệ thống cũng phát hiện các hoạt động đáng ngờ hoặc độc hại và tự động triển khai thêm các biện pháp khắc phục. Về khía cạnh sử dụng USB, việc kết hợp USB tùy chỉnh của Kingston Technology giúp đảm bảo có thể xác định danh sách các thiết bị được cho phép một cách dễ dàng nhất, đồng thời dữ liệu được mã hóa bằng phương pháp có thể truy nguyên. Nhờ đó, khả năng tuân thủ được tăng cường đáng kể mà không hề tốn thêm công sức.



“ Với chức năng của phần mềm bảo vệ dữ liệu EgoSecure và tính năng xác định danh sách các thiết bị được cho phép, chúng tôi chỉ cho phép phê duyệt các USB được mã hóa của Kingston. Chúng tôi đưa các USB được mã hóa của Kingston vào danh sách những thiết bị được cho phép nhờ sử dụng ID phần cứng cá nhân hóa – và không cho phép các thiết bị khác. Điều này giúp giảm thiểu đáng kể nỗ lực quản trị, đồng thời tăng cường bảo mật dữ liệu! ”

Giám đốc CNTT, Công ty tài chính

Phần 4: Tình huống điển hình trong ngành Ô tô

Tình huống:

Trong ngành ô tô, nhiều lĩnh vực khác nhau sử dụng thiết bị USB. Ví dụ: dữ liệu nghiên cứu được lưu trữ trên các thiết bị lưu trữ bên ngoài và được trao đổi giữa các kỹ sư tương ứng của công ty. Để cấu hình máy móc sản xuất, các tệp được chuyển từ môi trường CNTT sang môi trường vận hành (OT). Toàn bộ những dữ liệu này đều rất nhạy cảm và phải được bảo vệ, tránh các nguy cơ gián điệp kinh tế và đánh cắp dữ liệu. Nếu không, các bí quyết mà doanh nghiệp tích lũy sẽ rơi vào tay kẻ xấu.

Thách thức:

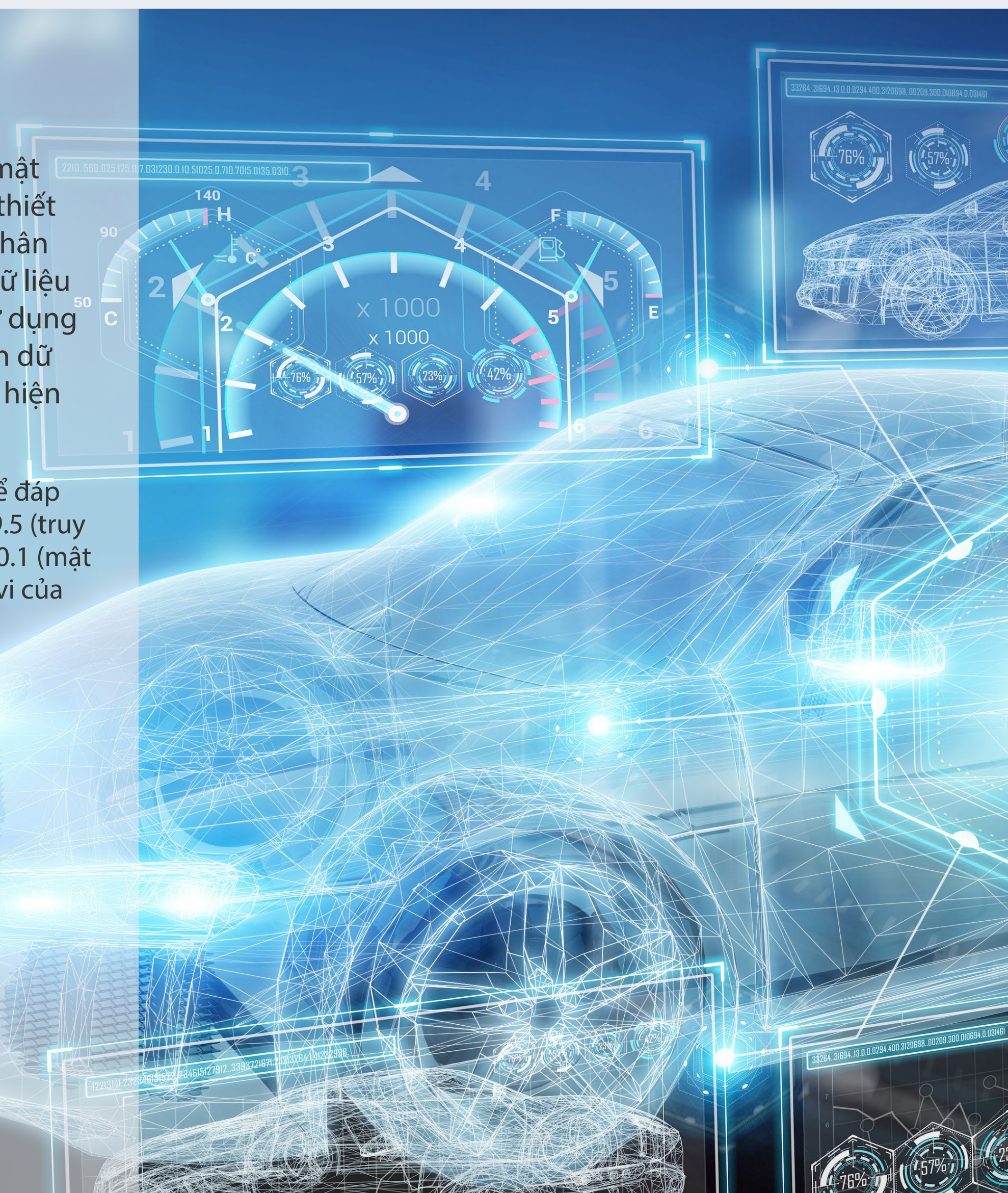
Ngành ô tô phải đáp ứng các yêu cầu tuân thủ như TISAX, bảo vệ nguyên mẫu, ENX, ISO27001, “kết nối với bên thứ ba” và GDPR. Theo quy định TISAX, các Điều khoản kiểm soát 9.1, 9.5 và 10.1 quy định rằng phải kiểm soát, giám sát, lọc và mã hóa các hoạt động truy cập dữ liệu. Ngoài ra, cũng phải tuân thủ các biện pháp này để đáp ứng những yêu cầu tuân thủ khác như GDPR và ISO27001 trong tất cả các lĩnh vực của doanh nghiệp ô tô.

Giải pháp:

Các USB được mã hóa của Kingston Technology bảo mật dữ liệu nhờ công nghệ mã hóa bằng phần cứng. Các thiết bị này có thể nhận được số sê-ri và ID phần cứng cá nhân hóa – có thể được sử dụng trong phần mềm bảo vệ dữ liệu EgoSecure để tự động lập danh sách các hình thức sử dụng dữ liệu cụ thể được cho phép. Ngoài ra, việc di chuyển dữ liệu cũng có thể được giám sát và phân tích nếu phát hiện hoạt động đáng ngờ.

“ Nhờ Matrix42 và Kingston Technology, chúng tôi có thể đáp ứng các yêu cầu của TISAX như điều khoản Kiểm soát 9.5 (truy cập thông tin và ứng dụng) và điều khoản Kiểm soát 10.1 (mật mã học) mà không gây ra những thay đổi lớn về hành vi của người dùng. ”

Giám đốc công nghệ, nhà cung cấp ô tô



Tình huống:

Các nhà cung cấp dịch vụ viễn thông nắm rất nhiều thông tin về khách hàng. Đây là những thông tin cực kỳ nhạy cảm, đặc biệt là theo quy định GDPR. Do đó, cần thực hiện đầy đủ các biện pháp để ngăn chặn nguy cơ thất lạc và đánh cắp dữ liệu.

Thách thức:

Hàng ngày, nhân viên của các công ty viễn thông đều xử lý dữ liệu của khách hàng. Hầu hết dữ liệu được lưu trữ trong các ứng dụng của doanh nghiệp. Tuy nhiên, vẫn có nguy cơ rằng hợp đồng của khách hàng hay thậm chí tệp xuất cơ sở dữ liệu được lưu trữ trên thiết bị đầu cuối và các thiết bị bên ngoài liên kết với chúng. Người dùng thường sử dụng bộ nhớ lưu trữ bên ngoài để trao đổi dữ liệu. Do đó, điều quan trọng là cần phát hiện, khắc phục hoặc bảo vệ các phương pháp lưu trữ dữ liệu không đúng cách.

Giải pháp:

Để đơn giản hóa quy trình mua hàng, bạn có thể nhanh chóng mua USB mã hóa của Kingston Technology có ID sản phẩm cá nhân hóa thông qua một danh sách các thiết bị được cho phép đã xác định trên phần mềm bảo vệ dữ liệu EgoSecure và được phân phối thông qua Danh mục dịch vụ

Matrix42. Có thể tự động xác định và khắc phục các tệp lưu trữ và xuất dữ liệu, trong đó có thể chứa thông tin nhạy cảm, bằng phương pháp “kiểm tra nội dung sâu” dựa trên công nghệ quét “dữ liệu đang được sử dụng” và “dữ liệu trên thiết bị lưu trữ”. Các hoạt động di chuyển dữ liệu được ghi nhật ký tập trung. Do đó, nhân viên có thể nhận được phần cứng mới để lưu trữ dữ liệu nhanh chóng sau khi yêu cầu phần cứng và yêu cầu của họ được phê duyệt. Điều này có thể đảm bảo tuân thủ quy định GDPR.

“ Nhờ cổng thông tin tự phục vụ của Matrix42, người dùng của chúng tôi có thể yêu cầu phương tiện lưu trữ khi cần. Sau khi đơn hàng được phê duyệt và giao đến khách hàng, thiết bị này sẽ được cho phép trên tính năng điều khiển thiết bị của EgoSecure. Sự kết hợp giữa Matrix42 và Kingston Technology đã giúp công ty chúng tôi tăng năng suất và khả năng bảo mật. ”

**Giám đốc công nghệ,
Nhà cung cấp dịch vụ viễn thông**



Phần 6: Tình huống điển hình trong ngành Ngành sản xuất



Tình huống:

Dữ liệu kỹ thuật số là kho báu của tương lai. Những dữ liệu đáng giá trong các ngành sản xuất bao gồm kế hoạch sản xuất, dữ liệu về khách hàng và nhà cung cấp cũng như bí quyết của công ty. Sự cố thất lạc dữ liệu không những khiến doanh nghiệp phải chịu các hình phạt rất nặng theo quy định GDPR mà còn gặp phải các vấn đề về danh tiếng, với mức độ nghiêm trọng khôn lường. Thật không may, USB xuất hiện đầy rẫy hàng ngày trên taxi, tại tiệm giặt là, ở sân bay, ga tàu hoặc bãi đậu xe.

Thách thức:

Các thiết bị lưu trữ thường chứa dữ liệu cực kỳ nhạy cảm và thật không may, dữ liệu này thường không được mã hóa. Ngoài ra, còn có nguy cơ khi các kỹ thuật viên dịch vụ sử dụng thiết bị truyền dữ liệu bên ngoài để cài đặt các bản cập nhật cho máy móc sản xuất. Các thiết bị bên ngoài này có nguy cơ để lọt phần mềm độc hại vào mạng nội bộ.

Giải pháp:

Các USB được mã hóa của Kingston Technology bảo mật dữ liệu nhờ công nghệ mã hóa bằng phần cứng. Các thiết bị này có thể được cấp số sê-ri và ID phần cứng cá nhân hóa – có thể được sử dụng trong phần mềm bảo vệ dữ liệu EgoSecure để tự động lập danh sách các hình thức sử dụng dữ liệu cụ thể được cho phép. Ngoài ra, việc di chuyển dữ liệu cũng có thể được giám sát và phân tích nếu phát hiện hoạt động đáng ngờ.

“Mã hóa dữ liệu sản xuất có vai trò rất quan trọng trong việc bảo vệ chúng tôi khỏi nguy cơ đánh cắp dữ liệu. Dữ liệu cực kỳ nhạy cảm này chỉ được cho phép trên các USB Kingston mã hóa đã được phê duyệt thông qua tính năng lọc tệp của phần mềm bảo vệ dữ liệu EgoSecure. Trên tất cả các thiết bị USB khác, dữ liệu sản xuất bị chặn và quyền ghi vào các bộ lưu trữ dữ liệu bên ngoài được bảo mật bằng tính năng ghi nhật ký và mã hóa nhanh của EgoSecure.”

Giám đốc bảo mật CNTT, Ngành sản xuất





Phần 7: Các giải pháp của Kingston Technology và Matrix42



Việc sử dụng công nghệ mã hóa, bộ nhớ và thiết bị lưu trữ nhanh kết hợp với các tiêu chuẩn, chính sách và các quy tắc thực hành tốt nhất là một bước tiến lớn. Máy tính xách tay và USB bị thất lạc khiến cho các cá nhân và công ty đều dễ bị tổn thương trước sự cố làm lộ thông tin cá nhân và riêng tư. Kingston Technology cung cấp các giải pháp ngăn ngừa mối đe dọa để giúp giảm thiểu nguy cơ, đồng thời bổ sung cho một kế hoạch bảo mật hiện có hoặc đang được phát triển.

USB Mã hóa của Kingston Technology

USB mã hóa bằng phần cứng của Kingston Technology trang bị các giải pháp bảo vệ dữ liệu cho dữ liệu di động bên trong và bên ngoài tường lửa của một tổ chức. Được thiết kế để bảo vệ dữ liệu đòi hỏi bảo mật nghiêm ngặt, những ổ này giúp bạn đáp ứng các tiêu chuẩn ngành, chỉ thị và quy định cụ thể. Các sản phẩm đều tuân thủ quy định TAA, đạt chứng nhận FIPS và hiện có nhiều mức dung lượng, tối đa là 128 GB. Nhờ đó, chúng rất lý tưởng cho cả người dùng doanh nghiệp và các cơ quan chính phủ.



Chương trình tùy chỉnh bảo mật

Bạn có thể tùy chỉnh USB mã hóa của Kingston Technology theo nhiều cách khác nhau để đáp ứng nhu cầu của công ty bạn. Hãy thêm các tính năng được chọn để có được USB thiết yếu và chỉ bạn mới có. Kingston Technology hỗ trợ đặt hàng USB mã hóa tùy chỉnh rất dễ dàng và thuận tiện thông qua đại lý mà bạn chỉ định. Dòng sản phẩm USB mã hóa của Kingston Technology gồm có DTVP30, DT4000G2 và IKD300S. Chương trình này mang đến những tùy chọn thường được khách hàng yêu cầu, bao gồm đánh số sê-ri, mặt khấu kép và logo tùy chỉnh. Với yêu cầu đơn hàng tối thiểu là 50 sản phẩm trong lần đặt hàng đầu tiên và 25 sản phẩm trong các lần đặt hàng tiếp theo, chương trình này đáp ứng đúng nhu cầu của công ty bạn.

Phần mềm bảo vệ dữ liệu EgoSecure của Matrix42

Phần mềm bảo vệ dữ liệu EgoSecure của Matrix42 cung cấp cho các công ty khả năng quản lý bảo mật 360° nhằm ngăn chặn sự cố và bảo vệ thiết bị, hệ thống và dữ liệu. Giải pháp này tự động hóa toàn bộ quy trình, từ ngăn chặn và phát hiện, cho đến các biện pháp đối phó trong trường hợp xảy ra thiệt hại, mà không hề gây mất năng suất.

Bảo vệ dữ liệu và an ninh mạng có vẻ là một trách nhiệm nặng nề. Những yêu cầu đối với công việc kỹ thuật số đã thay đổi đáng kể khi nhân viên có khả năng tự quyết định thời gian, địa điểm làm việc và thiết bị họ sử dụng trong công việc. Sự kết hợp chính xác giữa USB mã hóa bằng phần cứng với công nghệ quản lý phần mềm trên thiết bị đầu cuối có thể giúp các công ty nắm quyền kiểm soát các thiết bị trong doanh nghiệp của họ. Do đó, họ có thể giảm nguy cơ vi phạm dữ liệu và hỗ trợ duy trì chiến lược tuân thủ GDPR của mình.





Giới thiệu về Kingston

Với hơn 30 năm kinh nghiệm, Kingston Technology có kiến thức để xác định và giải quyết những thách thức bảo mật trên thiết bị đầu cuối mà bạn phải đối mặt và không hề gây ảnh hưởng đến tổ chức của bạn.

©2021 Kingston Technology Far East Corp. (Asia Headquarters) No. 1-5, Li-Hsin Rd. 1, Science Park, Hsin Chu, Taiwan.
Các nhãn hiệu thương mại đã đăng ký và các nhãn hiệu thương mại là tài sản của các chủ sở hữu tương ứng.

#KingstonIsWithYou