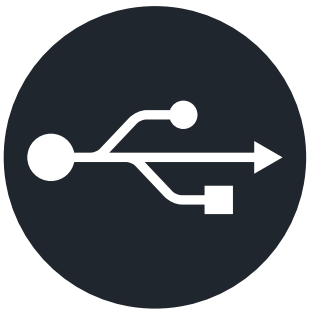
Cách cho phép truy cập USB
mà không ảnh hưởng đến bảo mật điểm cuối

#KingstonIsWithYou #KingstonIronkey

Giới thiệu

Vào tháng 1 năm 1996, thông số kỹ thuật chính thức của USB 1.0 đã được ra mắt và hứa hẹn tạo nên một kỷ nguyên của tính đồng nhất, tiện lợi và linh hoạt cho các nhà cung cấp thiết bị ngoại vi cũng như người dùng cuối. 27 năm sau, USB vẫn duy trì khả năng tương thích ngược với từng phiên bản. USB tiếp tục tồn tại và trở thành nền tảng của giao diện phần cứng máy tính, từ máy chủ đến điện thoại thông minh.



Tính đơn giản chỉ cần cắm và chạy, cùng tốc độ ngày càng tăng đã khiến ổ lưu trữ di động USB phát triển trở thành một trong những sáng kiến thành công nhất trong lịch sử. Thế nhưng, đi kèm tính tiện lợi đó là một sự đánh đổi trong bảo mật dữ liệu. Trong thế giới ngày nay, nếu không sử dụng các công cụ thích hợp như bảo vệ điểm cuối trên máy tính chủ và các phương pháp bảo mật dữ liệu thích hợp, người dùng có thái độ bất cẩn trong việc sử dụng ổ lưu trữ USB dễ mang theo sẽ khiến bản thân và những người khác có nguy cơ bị xâm phạm dữ liệu – một việc có thể gây tổn thất nặng nề cho người dùng cuối và thậm chí có thể làm tổn hại đến toàn bộ tổ chức hoặc chính phủ.

Ngoài việc bảo vệ môi trường máy chủ, USB cũng cần được bảo vệ bằng mật khẩu và tính năng mã hóa phần cứng trên thiết bị. Điều này tạo ra hàng rào phòng thủ chắc chắn nhất để chống lại xâm nhập. Chúng ta sẽ xem xét một số quy tắc thực hành tốt nhất để sử dụng USB an toàn hơn, cũng như có cái nhìn sâu hơn về USB nói chung.

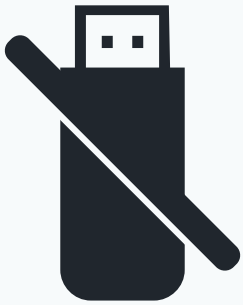
Biện pháp lý tưởng là sử dụng phương pháp kết hợp, nhưng độ vững chãi của tính năng mã hóa và cấu phần phần cứng nội tại của USB mới là điều tối quan trọng. Các yếu tố này mang lại lợi ích cho nhiều lĩnh vực từ tài chính, y tế đến sản xuất và quân sự. Các yếu tố này cũng đóng một vai trò quan trọng trong quá trình làm việc từ xa khi mà việc truy cập mạng là không khả dụng, dễ bị tấn công hoặc không thực tế.

Các USB mã hóa phần cứng hiện được cung cấp theo các xếp hạng chứng nhận khác nhau và cung cấp nhiều tính năng bảo mật. Bằng cách kiểm tra các thuộc tính và khả năng tùy chỉnh, tính phù hợp của USB để sử dụng làm các giải pháp độc lập cũng được thể hiện qua khả năng đảm bảo an toàn trong rất nhiều loại môi trường nhạy cảm khác nhau.

Cho phép truy cập cổng: Lưu trữ USB kết hợp với phần mềm chống thất thoát dữ liệu quản lý điểm cuối

Trong nhiều thập kỷ, các ứng dụng chống vi-rút và phần mềm độc hại đã tạo ra hàng rào bảo vệ ở cấp độ cơ bản nhất – tự động quét các tệp tin tải xuống và thiết bị đính kèm, đồng thời báo cáo hoặc có hành động đối với nội dung đáng ngờ. Khả năng bảo vệ của phần mềm chống vi-rút thế hệ mới (NGAV) sẽ tiến thêm một bước. Thay vì chỉ dựa vào cơ sở dữ liệu được cập nhật liên tục về các chữ ký vi-rút, NGAV bổ sung các tính năng học máy và phát hiện hành vi để có thể xác định và giảm thiểu các mối đe dọa chưa biết.

Tuy nhiên, đây không phải là vũ khí duy nhất. Đối với những người muốn thiết lập hàng rào bảo vệ chắc chắn khỏi các thiết bị ngoại vi của người dùng và nhiều loại khác, phần mềm Chống thất thoát dữ liệu quản lý điểm cuối (DLP) cung cấp phương tiện để từ chối bất kỳ loại truy cập nào vào cổng USB và các điểm truy cập khác.



Phương pháp "Chặn mọi cổng" để đảm bảo bảo mật chắc chắn có thể loại trừ rủi ro và, trong một số trường hợp, có thể là một giải pháp cần thiết. Tuy nhiên, thực tế cho thấy một chính sách như vậy thường không phải là một công cụ hiệu quả và có thể gây ra những hậu quả không mong muốn.

Dù vậy, một số quản trị viên CNTT thường từ chối yêu cầu mở cổng USB trên máy người dùng, vì làm như vậy trên các điểm cuối này sẽ cho phép truy cập trực tiếp vượt qua tường lửa của doanh nghiệp. Thái độ thận trọng đó là dễ hiểu, nhưng trong vấn đề cho phép truy cập ổ lưu trữ USB, việc cấp đặc quyền này không nhất thiết phải là rắc rối bảo mật lớn nếu tuân thủ các điều kiện tiên quyết nhất định.

Một yêu cầu thiết yếu là bộ ứng dụng quản lý điểm cuối phải có tính năng quét phát hiện mối đe dọa trên các giải pháp diệt vi-rút/chống phần mềm độc hại, cũng như giám sát và quản lý tập trung tất cả các điểm cuối của người dùng.

Nhìn chung, phương pháp đơn giản này xuất hiện dưới nhiều hình thức khác nhau trong những giải pháp hợp nhất của các nhà cung cấp phổ biến như McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection và WinMagic SecureDoc, v.v.

Tinh chỉnh danh sách trắng

Trong bảo mật các thiết bị lưu trữ USB, phương pháp cần triển khai phụ thuộc vào mức độ bảo vệ cần thiết. Một phương pháp đơn giản nhưng hiệu quả là đưa các thiết bị lưu trữ USB vào danh sách trắng bằng cách sử dụng các giá trị Mã nhận diện nhà cung cấp (VID) và Mã nhận diện sản phẩm (PID) tương ứng. Tất cả các thiết bị ngoại vi USB của mỗi nhà sản xuất đều có một mã VID duy nhất chung, nhưng mã PID sẽ thay đổi cho mỗi sản phẩm mới được phát hành.

Khi lập danh sách trắng, chỉ sử dụng mã VID của một nhà sản xuất sẽ là quá rộng để có thể bảo mật vì khi đó, mọi thiết bị USB mà đơn vị đó từng sản xuất đều sẽ được phép truy cập. Mã PID sẽ cho phép đi sâu vào từng sản phẩm hơn và yêu cầu chỉ một model cụ thể mới được cấp quyền truy cập vào hệ thống máy chủ.

Đây có thể là một bước cải tiến nhưng vẫn chưa phải là lý tưởng. Thiết bị lưu trữ USB cực kỳ phổ biến nên người dùng vẫn có thể mua thiết bị riêng sao cho giống với các model được cấp quyền. Trước những thách thức này, Kingston Technology cung cấp các giải pháp riêng để tăng cường bảo mật cho thiết bị lưu trữ USB của bạn.

Chương trình tùy chỉnh của chúng tôi sẽ tạo lập cấu hình PID tùy chỉnh dành riêng cho một tổ chức và áp dụng được cho nhiều loại ổ USB flash mã hóa của Kingston. Khi triển khai các thiết bị có mã nhận diện sản phẩm tùy biến này, các công ty không chỉ hưởng lợi từ một danh sách trắng được đơn giản hóa, mà còn có thể tăng cường đáng kể khả năng bảo mật. Nếu không có mã PID tùy chỉnh khớp với danh sách, ngay cả những thiết bị có vẻ giống hệt nhau do nhân viên tự mua cũng sẽ bị từ chối quyền truy cập.

Mặc dù mã PID tùy chỉnh sẽ cho phép quản trị viên CNTT đưa các thiết bị lưu trữ USB mới vào sử dụng thật nhanh chóng và dễ dàng, nhưng có một giải pháp thay thế ở cấp độ sâu hơn là sử dụng số sê-ri riêng của từng thiết bị mà hầu hết các USB

mã hóa của Kingston đều có. Giải pháp này yêu cầu phải đăng ký từng số sê-ri thiết bị duy nhất với bộ phần mềm quản lý điểm cuối. Ban đầu, việc này sẽ do nhân viên CNTT xử lý và Kingston có thể cung cấp danh sách các số sê-ri kèm mỗi đơn đặt hàng – các số này luôn ở dạng chữ và số và không theo thứ tự. Phương pháp này cho phép triển khai các chính sách linh hoạt hơn nhiều nhờ dựa trên quyền sở hữu ổ đĩa riêng lẻ, thêm vào đó là khả năng truy xuất nguồn gốc thiết bị chính xác – một lợi ích vô cùng giá trị trong các tình huống điều tra về CNTT. Một số ổ Kingston có sẵn số sê-ri và mã vạch trên vỏ để quét điện tử. Các ổ khác có thể được tùy chỉnh để thêm mã vạch và số sê-ri trên vỏ cho doanh nghiệp. Những thông tin này có thể được sử dụng để theo dõi ổ đĩa.

Theo mặc định, hệ thống quản lý điểm cuối cung cấp quyền truy cập vào mã VID/PID để chặn cổng và lập danh sách trắng. Giải pháp của Kingston giúp tận dụng các tính năng này linh hoạt hơn và cho phép triển khai các chính sách phù hợp và sáng tạo hơn, tạo điều kiện sử dụng thiết bị lưu trữ USB thuận lợi. Bằng cách thiết lập một phương pháp nhận dạng thích hợp, chính sách bao trùm "Chặn mọi cổng" không chỉ quá đơn giản mà còn trở nên thừa thãi.

Giải pháp an toàn và tuân thủ cho người dùng từ xa

Để đáp ứng nhu cầu bảo mật, việc lập danh sách trắng các thiết bị chỉ giúp giải quyết một nửa vấn đề, hay nói cách khác chỉ là giải pháp nửa vời.

Nhờ đặc tính tiện lợi và đơn giản, các thiết bị lưu trữ USB trở thành thứ không thể thiếu trong nhiều doanh nghiệp và tổ chức, nơi mà tính di động là chìa khóa để mang lại trải nghiệm truyền dữ liệu mượt mà. Trong hầu hết các môi trường, vì lý do tuân thủ và duy trì tốt "vệ sinh" CNTT, việc trang bị cho nhân viên USB mã hóa để phục vụ các tác vụ như vậy là điều cần thiết. Thông qua kết hợp bảo vệ bằng mật khẩu và mã hóa thiết bị, ổ lưu trữ di động sẽ được trang bị các biện pháp bảo vệ để ngăn truy cập vào dữ liệu nhạy cảm nếu thiết bị không may bị thất lạc, mất cắp hoặc bỏ quên trong trường hợp có khả năng dễ bị tấn công.

Đây không phải là một giải pháp đa năng vì có nhiều kỹ thuật mã hóa khác nhau và sự khác biệt trở nên đáng kể nhất khi so sánh giữa các giải pháp mã hóa phần mềm và phần cứng. Vậy giải pháp nào là tốt hơn? Điều này phụ thuộc vào nhu cầu của bạn, nhưng có một câu hỏi khó hơn cần giải đáp là: "Giải pháp nào an toàn hơn?"

Về cơ bản, mã hóa phần mềm là một lựa chọn giúp tiết kiệm ngân sách và có thể đáp ứng nhu cầu của một số lĩnh vực có quy mô hoạt động nhỏ. Giải pháp này cũng sẽ phù hợp với các doanh nghiệp không coi việc chuyển dữ liệu là hành động nhạy cảm và quan tâm nhiều hơn đến việc tuân thủ chính sách.

Tuy nhiên, mã hóa phần mềm cũng là điểm yếu của chính giải pháp này vì yêu cầu các ứng dụng tương tác trực tiếp với khách hàng cần phụ thuộc vào máy tính để thực hiện các tác vụ mã hóa. Do đó, khi liên kết, thiết bị lưu trữ được mã hóa bằng phần mềm chỉ có mức độ an toàn như máy tính chủ.

Khả năng bị khai thác cũng tăng cao vì nếu có quyền truy cập vào bộ nhớ của máy tính, tin tặc có thể "đánh hơi" được các mật khẩu mã hóa/giải mã. Dữ liệu trên ổ đĩa cũng có thể bị tấn công theo hình thức thử sai (brute force) vì tính năng bảo vệ truy cập bằng mật khẩu sẽ trở nên thừa thãi nếu có thể truy cập và sao chép các tệp được mã hóa.

Cần lưu ý rằng, mã hóa dựa trên phần mềm có thể đòi hỏi cập nhật phần mềm theo thời gian, điều này có thể khiến việc triển khai trở nên phức tạp do tạo thêm gánh nặng cho nhân viên CNTT. Điều tồi tệ nhất là mã hóa phần mềm có thể bị nhân viên gỡ bỏ hoàn toàn do chán nản với các vấn đề về tính di động của ổ nhớ giữa các nền tảng. Người dùng ổ nhớ có thể sao chép dữ liệu trên ổ đĩa mã hóa vào máy tính, định dạng lại ổ đĩa thành ổ đĩa không mã hóa, sau đó sao chép dữ liệu trở lại vào ổ đĩa. Lúc này, dữ liệu sẽ không được bảo mật và rất dễ bị xâm phạm. Đối với mục đích tuân thủ luật và quy định về quyền riêng tư dữ liệu, đây là hành vi không thể chấp nhận vì tính năng bảo mật của USB có thể hoàn toàn bị vô hiệu hóa.

Mã hóa trên chip: giải pháp chắc chắn và nhanh chóng

Ngược lại, USB được mã hóa phần cứng hoạt động độc lập với máy tính vì có bộ xử lý chuyên dụng được tích hợp sẵn trên ổ đĩa thực để quản lý quá trình mã hóa. Loại ổ này có một quy trình mã hóa luôn bật cùng khả năng bảo vệ chống lại các cuộc tấn công mật khẩu dạng thử sai, nhờ đó sẽ không cho phép truy cập và sao chép các dữ liệu được mã hóa.

Các USB mã hóa phần cứng cấp doanh nghiệp và cấp quân sự của Kingston sử dụng chuẩn mã hóa AES 256 bit ở chế độ XTS. Là một kỹ thuật mã hóa được chấp thuận trên toàn cầu, AES 256 bit mang đến các biện pháp bảo vệ dữ liệu nghiêm ngặt. Bằng cách sử dụng hai mật khẩu riêng biệt ở các giai đoạn khác nhau của quá trình mã hóa/giải mã, chế độ XTS có tác dụng tương tự như mã hóa dữ liệu hai lần.

Khi sử dụng, mật khẩu mã hóa được lấy từ trình tạo số ngẫu nhiên của bộ điều khiển ổ đĩa và cần mật khẩu của người dùng để mở khóa. Khi quá trình xác thực diễn ra trong phần cứng mật mã của thiết bị, mật khẩu mã hóa và các chức năng bảo mật quan trọng khác được bảo vệ chống lại các hành vi lợi dụng phổ biến như BadUSB, các cuộc tấn công khởi động nguội, mã độc hại và tấn công thử sai.

Một trong những lợi ích tức thì nhất của mã hóa phần cứng là hiệu suất của ổ đĩa được tăng cường đáng kể so với ổ đĩa được mã hóa phần mềm vì không phải tải các tác vụ mã hóa lên máy tính chủ. Mọi hoạt động đều diễn ra bên trong ổ đĩa.

Các USB được mã hóa phần cứng như Kingston IronKey D500S là thiết bị được bảo vệ bằng mật khẩu và đã được mã hóa sẵn. Khi sử dụng, chỉ có ổ khởi chạy được bảo vệ chống ghi mới hiển thị khi bắt đầu vì ổ này chứa ứng dụng được sử dụng để xác thực mật khẩu và mở khóa ổ lưu trữ được mã hóa chính. Quy trình này giúp tránh việc cài đặt bất kỳ loại trình điều khiển hoặc phần mềm nào trên máy tính chủ.

Hơn nữa, USB mã hóa phần cứng của Kingston được trang bị chương trình điều khiển có chữ ký số, giúp ngăn chặn mọi hành vi xâm phạm chương trình điều khiển trong thiết bị. Lớp bảo mật bổ sung này giúp bảo vệ chống lại các cuộc tấn công như BadUSB muốn khai thác lỗ hổng vốn có trong chương trình điều khiển của thiết bị USB. Điều này có thể khởi chạy các lệnh thực thi ẩn hoặc mã độc hại trên máy chủ.

Tất nhiên, phương pháp "Chặn mọi cổng" sẽ hạn chế rủi ro bị các cuộc tấn công BadUSB lợi dụng, nhưng sao phải hy sinh năng suất bằng các phương pháp lỗi thời như vậy? Như chúng tôi đã nhấn mạnh ở trên, hoàn toàn có thể vừa duy trì một môi trường an toàn, vừa cho phép sử dụng thiết bị lưu trữ di động nếu có các quy trình thu mua và triển khai đơn giản để đưa loại USB mã hóa phần cứng vào sử dụng.

Làm việc từ xa an toàn và tuân thủ

Khi làm việc từ xa, các cá nhân không được bảo vệ trong môi trường làm việc an toàn của tổ chức, vì vậy cần có một chiến lược phù hợp hơn cũng như một cái nhìn mới hơn về các yếu tố cần ưu tiên.

Trong một kế hoạch bảo mật từ xa, nếu chặn các cổng USB trên máy tính xách tay của nhân viên chỉ để buộc họ truy cập vào máy chủ qua Internet để tải lên hoặc truy xuất tài liệu, việc này có mang lại lợi ích gì? Khi di chuyển, họ có thể chỉ tiếp cận được các kết nối Internet mở như điểm truy cập Wi-Fi không an toàn hoặc không đáng tin cậy. Điều này gây ra nhiều mối nguy hiểm và làm gia tăng đáng kể khả năng bị xâm phạm. Các mối đe dọa như chặn và giám

sát dữ liệu thông qua giả mạo, tấn công xen giữa (Man-In-the-Middle, MitM) và nghe trộm mạng chỉ là một số trong những phương pháp tấn công ngày càng tinh vi mà tội phạm mạng có thể lợi dụng. Ngay cả mạng VPN cũng đã bị ảnh hưởng.

Kết nối mạng Internet của tổ chức cũng chính là một điểm cuối khác và mức độ tiếp xúc thường xuyên cố hữu khiến kết nối này trở thành một điểm xâm nhập cực kỳ dễ bị tấn công và nhắm đến. Khi mở cho phép truy cập từ xa sẽ tạo ra những rủi ro bảo mật riêng, đặc biệt là khi liên quan đến dữ liệu nhạy cảm.

Việc ủy thác cho nhân viên làm việc từ xa sử dụng USB được bảo vệ bằng mật khẩu và mã hóa phần cứng giúp loại bỏ hiệu quả các lỗ hổng mạng tiềm ẩn đó. Tuy nhiên, quá trình này đòi hỏi phải kiểm tra kỹ hơn các USB có thể sử dụng và xem các USB này đáp ứng nhu cầu của từng môi trường làm việc từ xa ra sao. Việc này không chỉ đơn giản là lựa chọn mức dung lượng của ổ đĩa hay quyết định có cần gán số sê-ri cho ổ đĩa hay không, mà liên quan đến cấu trúc vật lý của chính thiết bị.

Bảo vệ chống giả mạo: Giải pháp phần cứng vật lý

Vấn đề chính là cần xác định USB mã hóa phần cứng có tính năng chống tác động từ bên ngoài hay không. Mức độ an toàn của thiết bị trước những can thiệp như vậy được phản ánh ở các tiêu chuẩn như FIPS 140-3. Một số cấp độ của các tiêu chuẩn này nghiên cứu kỹ lưỡng khả năng chống chịu của cấu trúc vật lý của ổ đĩa khi không sử dụng các phương pháp mật mã.

Chứng nhận FIPS-197 liên quan chỉ đánh giá các thuộc tính mã hóa phần cứng và các thiết bị như IronKey Vault Privacy 50 và Ổ SSD Vault Privacy 80 External, đây là các mẫu dành cho doanh nghiệp và không yêu cầu bảo mật dữ liệu ở cấp quân sự. Những ổ đĩa này rẻ hơn nhưng thiếu khả năng bảo vệ chống lại hành vi giả mạo ổ đĩa vật lý.

Với chứng nhận FIPS 140-3 Cấp 3 (đang chờ phê duyệt), các phương pháp được triển khai để phát hiện hành vi giả mạo thiết bị được xếp hạng cấp quân sự. Kingston cung cấp các ổ FIPS 140-3 Cấp 3 này cho các doanh nghiệp, chính phủ và quân đội trên toàn thế giới.

Sử dụng nhựa epoxy bên trong để phủ lên tất cả các mạch ổ đĩa cần bảo mật và gắn chặt các cấu phần bên trong vào vỏ là biện pháp tạo ra một bức tường bảo vệ khác. Mọi nỗ lực mở vỏ kim loại đều sẽ cực kỳ khó khăn và có thể khiến các chip và các cấu phần khác bên trong bị hư vỡ, cuối cùng khiến ổ đĩa không thể hoạt động. Với loại nhựa epoxy cứng và không trong suốt này, việc giả mạo các cấu phần quan trọng trở thành một nhiệm vụ gần như bất khả thi. Các thiết bị như Kingston IronKey D500S và S1000 có tính năng bảo mật bổ sung này.

Không chỉ giới hạn ở các biện pháp bảo vệ thiết bị mang tính vật lý, Kingston IronKey S1000 còn nâng khả năng chống giả mạo lên một cấp độ cao hơn. Chip mật mã trong của IronKey S1000 có thể phát hiện ra bất kỳ hành vi giả mạo vật lý nào và sẽ khiến ổ đĩa không thể sử dụng được ngay sau khi thiết bị được khởi động. Trông cậy vào các thiết bị lưu trữ USB mã hóa phần cứng để truy cập và truyền các tệp nhạy cảm là một giải pháp thực tế, tạo điều kiện cho các hoạt động từ xa được diễn ra dễ dàng và đảm bảo duy trì bảo mật tại chỗ hiệu quả.

Bạn nên nghiên cứu về phần cứng và các tính năng bảo mật của USB để xem liệu các USB này có phù hợp với nhu cầu và trường hợp sử dụng cụ thể của bạn hay không. Mỗi USB đều cần được xem xét theo từng trường hợp cụ thể dựa trên các chứng nhận đáng tin cậy để tạo căn cứ cho quyết định của bạn. Dù ưu tiên của bạn là gì, Kingston đều có thể đáp ứng với một loạt các giải pháp USB mã hóa phần cứng và các tùy chọn tùy chỉnh với mức giá phải chăng, phù hợp với mọi môi trường: từ tuân thủ chung cho đến các thông số kỹ thuật quân sự khắt khe nhất.

An toàn là trên hết: Không kết nối mạng thì sẽ không có vấn đề

Ngày nay, khi không gian làm việc không chỉ giới hạn ở văn phòng và xu hướng làm việc tại nhà tiếp tục phát triển, thì các vấn đề về lỗ hổng truy cập từ xa trở thành tiêu điểm cho nhiều công ty. Nhiều công ty đang lần đầu tiên phải đối mặt với những thách thức này và đang tìm kiếm những cách thức an toàn hơn để thích ứng với xu hướng ngày một phát triển này.

Để hỗ trợ những nhu cầu này trong nhiều ngành, các thiết bị lưu trữ USB mã hóa phần cứng đã được phát triển đầy đủ và cung cấp một giải pháp an toàn cho những tình huống không thể hoặc không mong muốn truyền dữ liệu qua mạng vì một số lý do.

Trong lĩnh lực tài chính, các cơ quan quản lý thường yêu cầu xem dữ liệu để kiểm tra hành vi và sự tuân thủ của một công ty. Rủi ro bị xâm phạm là quá lớn, khiến chúng ta e dè việc chuyển qua mạng các tài liệu nhạy cảm có chứa thông tin chi tiết chính xác về các khoản đầu tư, giao dịch thị trường và các hoạt động ngân hàng bí mật khác. Giải pháp đơn giản và hiệu quả là chuyển những thông tin này qua USB được mã hóa phần cứng.

Sử dụng USB bảo mật để truyền tệp trong lĩnh vực y tế là hoạt động diễn ra hàng ngày. Việc này cũng nhằm tạo thuận tiện cho các bác sĩ hoặc nhà tư vấn khi muốn phân tích các tệp, tham khảo để nghiên cứu hoặc trình bày các ví dụ điển hình cho sinh viên y khoa. Đối với các hệ thống độc quyền như thiết bị chụp ảnh y khoa, nhu cầu này trở nên thực tế hơn khi mà quyền truy cập mạng là không khả dụng hoặc không an toàn. Bằng cách sử dụng USB mã hóa phần cứng phù hợp, người dùng có thể dễ dàng chuyển các tệp để sử dụng ở nơi khác.

Những điều nên và không nên

✓ **Sử dụng các ổ đĩa an toàn, tuân thủ** và xem xét các thông số kỹ thuật khi mua sao cho phù hợp với nhu cầu của mỗi tình huống triển khai.

✗ **Không cho phép thực hiện chính sách Mang thiết bị của riêng bạn (BYOD) áp dụng ngẫu nhiên hoặc theo cá nhân** – đối với bất kỳ công ty nào, việc mất các ổ đĩa không được mã hóa là một cái giá quá đắt về mặt tài chính và danh tiếng.

✓ **Triển khai bộ ứng dụng quản lý điểm cuối,** đồng thời sử dụng USB được mã hóa phần cứng và có cung cấp các tính năng danh sách trắng đặc biệt.

✗ **Đừng phụ thuộc vào may rủi.** Đánh giá cẩn thận các yêu cầu đối với môi trường làm việc tại chỗ và từ xa.

✓ **Cung cấp kiến thức cho nhân viên** về các vấn đề bảo mật. Bảo vệ công ty trước các hành vi xâm phạm bảo mật là vì lợi ích của chính họ.

✗ **Đừng làm cho vấn đề bảo mật trở nên khó khăn** đến mức người dùng tìm kiếm các giải pháp đường vòng có thể dẫn đến giảm tác dụng của các giải pháp CNTT được áp dụng. Một chính sách bao trùm vẫn luôn được áp dụng không có nghĩa là chính sách đó sẽ phù hợp với mọi tình huống. Môi trường làm việc đang ngày một thay đổi và bằng cách lựa chọn các giải pháp phù hợp, các công ty sẽ có thể phát triển và thực thi những chính sách mới.

Trong trường hợp này, Kingston IronKey Keypad 200 (KP200) là giải pháp đặc biệt hữu dụng. Đây là một ổ đĩa độc lập với hệ điều hành và không có bộ trình khởi chạy để nhập mật khẩu, mà thay vào đó có bàn phím chữ và số sử dụng để mở khóa thiết bị trên mọi nền tảng. Giống như một con dao đa năng dành cho các USB mã hóa phần cứng, thiết bị này còn mở rộng phạm vi ứng dụng sang lĩnh vực sản xuất; chuyển giao an toàn các ứng dụng được tạo ra trong môi trường nghiên cứu và phát triển CNTT sang các máy móc được điều khiển bằng nền tảng công nghệ vận hành (OT). Đối với các hoạt động trên nền tảng hỗn hợp vận hành cả trên Linux, KP200 là một trong những giải pháp bảo mật dễ sử dụng nhất hiện có.

Thiết bị lưu trữ USB được mã hóa phần cứng cũng đóng một vai trò quan trọng trong thực thi pháp luật. Các thiết bị lưu trữ USB này bảo vệ và chuyển giao an toàn hồ sơ vụ án, hình ảnh và các bằng chứng khác cho các nhân viên hiện trường, đội điều tra và đội pháp y. Các ổ đĩa của Kingston còn có thêm một lợi ích nữa vì các số sê-ri bên trong được in trên vỏ ngoài cùng với mã vạch. Quá trình phân phát và lập danh mục các ổ đĩa sẽ trở nên đơn giản và dễ theo dõi. Chỉ cần dễ dàng ghi số sê-ri một cách thủ công hoặc nhanh chóng quét mã vạch – nhờ đó, việc kiểm tra và quản lý kho thiết bị trở nên dễ dàng hơn bao giờ hết. Đây là tính năng tiêu chuẩn trên ổ Kingston IronKey D500S, D500SM và S1000B/E, nhưng cũng khả dụng ở các mẫu được mã hóa phần cứng khác thuộc phạm vi chương trình Tùy chỉnh của Kingston.

Tính di động trong bảo mật và lưu trữ: Giải pháp tối tân

Bảo vệ bằng mật khẩu, mã hóa phần cứng, bảo vệ chống tác động từ bên ngoài, danh sách điểm cuối chi tiết, chứng nhận cấp độ quân sự FIPS 140-3 cấp 3 (đang chờ phê duyệt) và nhật ký xem nhanh là những tính năng có sẵn của ổ USB Kingston để bạn có thể triển khai ngay mà không cần chờ thêm.

Các biện pháp bảo vệ bảo mật mạnh mẽ này đảm bảo rằng USB và dữ liệu bên trong luôn an toàn trong môi trường máy chủ. Mặc dù các thông số kỹ thuật được trình bày rất ấn tượng, nhưng nếu chỉ chọn một mẫu ngẫu nhiên mà không nghiên cứu có thể sẽ không mang lại giải pháp lý tưởng cho một số tổ chức có các yêu cầu khắt khe hơn.

Là một nhà sản xuất độc lập, Kingston cung cấp rất nhiều lựa chọn để đáp ứng nhu cầu của khách hàng. Thông qua chương trình Tùy chỉnh, Kingston mang đến các giải pháp nâng cao, được thiết kế để mang lại trải nghiệm trơn tru cho người dùng.

Tùy chỉnh an toàn có nhiều tính năng, chứ không chỉ là cung cấp mã PID USB cho riêng một tổ chức để đưa vào danh sách trắng. Hồ sơ bảo mật của ứng dụng trình khởi chạy cũng có thể được tùy chỉnh bằng cách sử dụng mười lăm tùy chọn khác nhau từ thông tin liên hệ và chi tiết công ty để bật gợi ý mật khẩu và xác định số lần thử mật khẩu tối đa. Đối với phần vỏ thiết bị, thương hiệu công ty (co-logo) cũng có thể được in sẵn, cùng một loạt các tùy chọn màu sắc cho các ổ đĩa cụ thể. Với đơn đặt hàng tối thiểu là năm mươi ổ đĩa, tất cả các tính năng này sẽ cung cấp khả năng tích hợp dễ dàng để triển khai thiết bị.

Nếu chưa có ứng dụng quản lý điểm cuối phù hợp để đảm bảo an toàn cho ổ lưu trữ USB, thì bạn có thể chọn một giải pháp quản lý dành cho các tổ chức muốn quản lý nhóm ổ đĩa Kingston, bao gồm các tùy chọn đặt lại mật khẩu từ xa.

Sự phổ biến và tiện lợi đã giúp USB tồn tại lâu hơn rất nhiều loại công nghệ hứa hẹn khác và đối với nhiều tác vụ thì tính tức thời và tiện lợi của USB vẫn sẽ là lợi thế. Luôn sẵn có và an toàn, loại USB được bảo vệ cung cấp một giải pháp đơn giản và hiệu quả cao.

Sao phải lo lắng về vi phạm dữ liệu mạng trong môi trường từ xa? Với các thiết bị lưu trữ USB được mã hóa phần cứng của Kingston IronKey, câu trả lời sẽ nằm trong tầm tay bạn.

Để tìm hiểu thêm về những gì Kingston có thể hỗ trợ, hãy truy cập kingston.com/ironkey hoặc để đặt các câu hỏi cụ thể hơn, hãy hỏi một trong những Chuyên gia USB mã hóa của chúng tôi.

#KingstonIsWithYou #KingstonIronkey