

Windows 10, 8.1, 8 và 7 đều bao gồm mã hóa ổ đĩa BitLocker, nhưng đó không phải là giải pháp mã hóa duy nhất họ cung cấp. Windows cũng bao gồm một phương thức mã hóa có tên là hệ thống tập tin mã hóa, hay còn gọi là EFS. Đây là cách nó khác với BitLocker.

Điều này chỉ có trên phiên bản Chuyên nghiệp và Doanh nghiệp của Windows. Các phiên bản tại nhà chỉ có thể sử dụng tính năng mã hóa thiết bị bị hạn chế nhiều hơn và chỉ khi đó là một PC hiện đại được cung cấp với mã hóa thiết bị được kích hoạt.

BitLocker là mã hóa toàn bộ đĩa

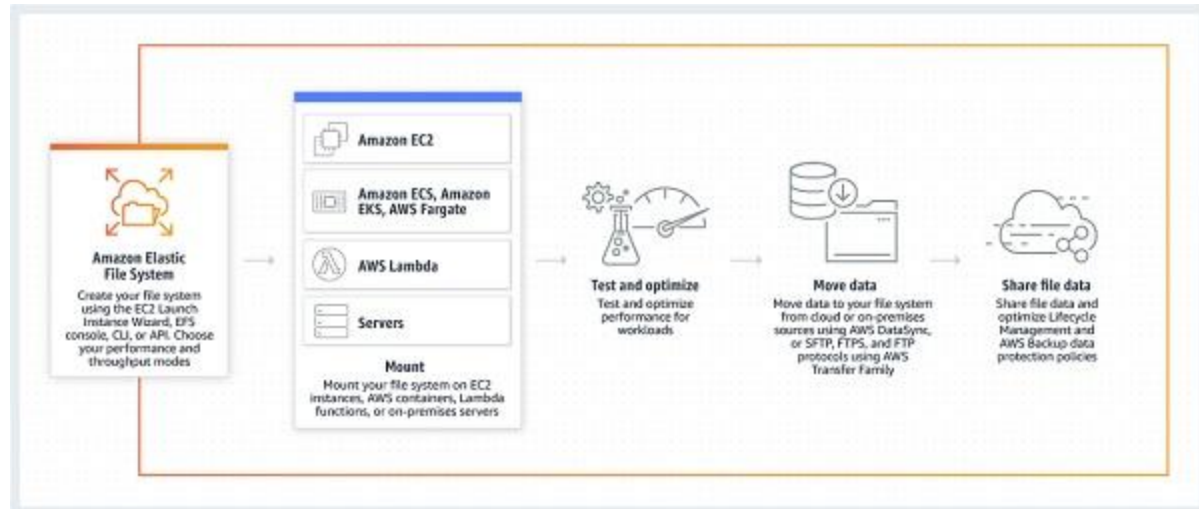
BitLocker là một giải pháp mã hóa toàn bộ đĩa mã hóa toàn bộ ổ đĩa. Khi bạn thiết lập BitLocker, bạn sẽ mã hóa toàn bộ phân vùng – chẳng hạn như phân vùng hệ thống Windows, phân vùng khác trên ổ đĩa trong hoặc thậm chí phân vùng trên ổ flash USB hoặc phương tiện bên ngoài khác.

Chỉ có thể mã hóa một vài tệp bằng BitLocker bằng cách tạo tệp chứa được mã hóa. Tuy nhiên, tệp chứa này thực chất là một hình ảnh đĩa ảo và BitLocker hoạt động bằng cách coi nó như một ổ đĩa và mã hóa toàn bộ.

Nếu bạn sẽ mã hóa ổ cứng để bảo vệ dữ liệu nhạy cảm khỏi rơi vào tay kẻ xấu, đặc biệt là nếu máy tính xách tay của bạn bị đánh cắp, BitLocker là cách tốt nhất. Nó sẽ mã hóa toàn bộ ổ đĩa và bạn sẽ không phải suy nghĩ về tệp tin nào được mã hóa và tệp tin nào không. Toàn bộ hệ thống sẽ được mã hóa.

Điều này không phụ thuộc vào tài khoản người dùng. Khi quản trị webnohu.comen kích hoạt BitLocker, mọi tài khoản người dùng trên PC sẽ được mã hóa các tệp của nó. BitLocker sử dụng mô-đun nền tảng đáng tin cậy của máy tính – hoặc TPM – phần cứng.

Mặc dù mã hóa ổ đĩa cứng, nhưng giới hạn của Windows trên Windows 10 và 8.1, nó hoạt động tương tự trên các PC có sẵn. Nó mã hóa toàn bộ ổ đĩa chứ không phải các tệp riêng lẻ trên đó.



EFS mã hóa các tệp riêng lẻ

EFS – hệ thống tập tin mã hóa mã hóa – hoạt động khác nhau. Thay vì mã hóa toàn bộ ổ đĩa của bạn, bạn sử dụng EFS để mã hóa từng tệp và thư mục riêng lẻ. Trong đó BitLocker là một bộ cài đặt và quên nó trong hệ thống của mình, EFS yêu cầu bạn chọn thủ công các tệp bạn muốn mã hóa và thay đổi cài đặt này.

Bạn làm điều này từ cửa sổ File Explorer. Chọn một thư mục hoặc các tệp riêng lẻ, mở cửa sổ Thuộc tính, nhấp vào nút Nâng cao nâng cao trong mục Thuộc tính và kích hoạt nội dung Mã hóa mã hóa để bảo mật dữ liệu tùy chọn.

Mã hóa này là trên cơ sở cho mỗi người dùng. Các tệp được mã hóa chỉ có thể được truy cập

bởi tài khoản người dùng cụ thể đã mã hóa chúng. Mã hóa là minh bạch. Nếu tài khoản người dùng đã mã hóa các tệp được đăng nhập, họ sẽ có thể truy cập các tệp mà không cần bất kỳ xác thực bổ sung nào. Nếu tài khoản người dùng khác được đăng nhập, các tệp sẽ không thể truy cập được.

Khóa mã hóa được lưu trữ trong chính hệ điều hành thay vì sử dụng phần cứng TPM của máy tính và kẻ tấn công có thể giải nén nó. Không có mã hóa toàn bộ ổ đĩa bảo vệ các tệp hệ thống cụ thể đó trừ khi bạn cũng bật BitLocker.

Cũng có khả năng các tập tin được mã hóa có thể bị rò rỉ ra các khu vực không được mã hóa. Ví dụ: nếu một chương trình tạo tệp bộ đệm tạm thời sau khi mở tài liệu được mã hóa EFS có thông tin tài chính nhạy cảm, tệp bộ đệm đó và dữ liệu nhạy cảm của nó sẽ được lưu trữ không được mã hóa trong một thư mục khác.

Trong đó BitLocker thực chất là một tính năng của Windows có thể mã hóa toàn bộ ổ đĩa, EFS tận dụng các tính năng trong chính hệ thống tệp NTFS.

Tại sao bạn nên sử dụng BitLocker chứ không phải EFS

Thực tế có thể sử dụng cả BitLocker và EFS cùng một lúc, vì chúng là các lớp mã hóa khác nhau. Bạn có thể mã hóa toàn bộ ổ đĩa của mình và thậm chí sau khi làm như vậy, người dùng Windows sẽ có thể kích hoạt thuộc tính Mã hóa mã hóa cho các tệp và thư mục. Tuy nhiên, thực sự không có nhiều lý do để làm như vậy.

Nếu bạn muốn mã hóa, tốt nhất nên sử dụng mã hóa toàn bộ đĩa dưới dạng BitLocker. Đây không chỉ là một bộ cài đặt và quên nó là giải pháp mà bạn có thể kích hoạt một lần và quên đi, nó còn an toàn hơn.

Chúng tôi có xu hướng phủ bóng lên EFS khi webnohu.com nói về mã hóa trên Windows và thường chỉ đề cập đến BitLocker là giải pháp mã hóa của Microsoft trên Windows. Có một lý do cho webnohu.com nói này. Mã hóa toàn bộ đĩa của BitLocker chỉ vượt trội so với EFS và bạn nên sử dụng BitLocker nếu bạn cần mã hóa.

Vậy tại sao EFS thậm chí còn tồn tại? Một lý do là đó là một tính năng cũ hơn của Windows.

BitLocker đã được giới thiệu cùng với Windows webnohu.com nói. EFS đã được giới thiệu trở lại trong Windows 2000.

Tại một thời điểm, BitLocker có thể đã làm chậm hiệu năng tổng thể của hệ điều hành, trong khi EFS sẽ nhẹ hơn một chút. Nhưng, với phần cứng hợp lý hiện đại, điều này hoàn toàn không nên xảy ra.

Chỉ cần sử dụng BitLocker và quên Windows thậm chí cung cấp EFS. Nó thực sự ít rắc rối để thực sự sử dụng và an toàn hơn.

The post [Amazon Elastic File System \(Efs Là Gì ? / Làm Thế Nào Để Định Nghĩa Và Giải Thích Ý Nghĩa](#) appeared first on [WEBNOHU](#).

Nguồn: WEBNOHU

<https://webnohu.com/amazon-elastic-file-system-efs-la-gi-lam-the-nao-de-dinh-nghia-va-giai-thich-h-y-nghia>