

















So sánh mã hóa bằng phần cứng và phần mềm

Hiểu những khác biệt chính và đâu là lựa chọn tốt hơn cho nhu cầu của bạn.



Trong cuộc chiến không ngừng nhằm bảo mật dữ liệu, sự khác biệt giữa mã hóa phần cứng và mã hóa phần mềm nằm ở việc bảo mật ở đâu và mức độ dễ bị phơi bày của nó trong môi trường sử dụng thực tế. Đối với các USB và SSD, nơi tích hợp mã hóa quyết định mức độ an toàn của dữ liệu cũng như mức độ phụ thuộc vào hệ thống xung quanh.

PHẦN CỨNG	SO SÁNH	PHẦN MỀM
 <p>Quản lý mật khẩu mã hóa Mật khẩu mã hóa được tạo ra bên trong phần cứng và được lưu trữ an toàn ngay trong ổ đĩa.</p>		 <p>Quản lý mật khẩu mã hóa Mật khẩu của người dùng được sử dụng trực tiếp làm mật khẩu mã hóa và các mật khẩu này có thể nằm trong bộ nhớ hệ thống.</p>
 <p>Bảo vệ chống tấn công dò mật khẩu Được thiết kế để bảo vệ chống lại các cuộc tấn công dò mật khẩu bằng cách giới hạn số lần thử trước khi ổ đĩa tự xóa dữ liệu, ngăn chặn bất kỳ ai truy cập dữ liệu nhạy cảm nếu ổ đĩa bị mất hoặc bị đánh cắp.</p>		 <p>Bảo vệ chống tấn công dò mật khẩu Do dễ bị tấn công vét cạn, máy tính sẽ cố gắng giới hạn số lần thử giải mã nhưng tin tặc có thể truy cập bộ nhớ máy tính và đặt lại bộ đếm lần thử.</p>
 <p>Yêu cầu phần mềm hoặc trình điều khiển Không cần cài đặt trình điều khiển hoặc phần mềm trên hệ thống máy chủ.</p>		 <p>Yêu cầu phần mềm hoặc trình điều khiển Yêu cầu cài đặt phần mềm, trình điều khiển và khả năng tương thích với hệ điều hành có thể khác nhau.</p>
 <p>Tài nguyên mã hóa Sử dụng bộ xử lý mật mã chuyên dụng được tích hợp ngay trong ổ đĩa.</p>		 <p>Tài nguyên mã hóa Sử dụng CPU và tài nguyên hệ thống của máy tính chủ để mã hóa và giải mã dữ liệu.</p>
 <p>Mức độ phụ thuộc và phơi bày với hệ thống máy chủ Cơ chế bảo mật được cô lập bên trong thiết bị và vẫn được bảo vệ ngay cả khi kết nối với các máy tính không đáng tin cậy hoặc đã bị nhiễm mã độc.</p>		 <p>Mức độ phụ thuộc và phơi bày với hệ thống máy chủ Bảo mật phụ thuộc vào hệ điều hành của máy chủ và dễ bị tổn thương hơn nếu máy tính bị nhiễm malware.</p>
 <p>Trạng thái mã hóa Mã hóa luôn được bật theo thiết kế và không thể gỡ bỏ hoặc bỏ qua.</p>		 <p>Trạng thái mã hóa Mã hóa có thể được bật, tắt hoặc cấu hình sai.</p>
 <p>Ảnh hưởng đến hiệu năng Ảnh hưởng tối thiểu đến hiệu năng, vì quá trình mã hóa được chuyển giao cho bộ xử lý phần cứng.</p>		 <p>Ảnh hưởng đến hiệu năng Có thể ảnh hưởng tiêu cực đến hiệu năng vì mã hóa sử dụng chung tài nguyên CPU.</p>
 <p>Khả năng linh hoạt Mã hóa gắn liền với chính ổ đĩa USB hoặc SSD cụ thể.</p>		 <p>Khả năng linh hoạt Có thể được triển khai trên hầu hết mọi loại phương tiện lưu trữ.</p>



Mã hóa phần mềm mang lại khả năng linh hoạt, trong khi mã hóa phần cứng giữ cho bảo mật được cô lập và ít bị ảnh hưởng bởi các rủi ro cấp hệ thống. Hiểu cách mỗi loại bảo vệ dữ liệu và kiểm soát quyền truy cập giúp bạn chọn mức độ bảo mật phù hợp với quá trình làm việc và hồ sơ rủi ro của mình.