**Windows Fundamentals 3**

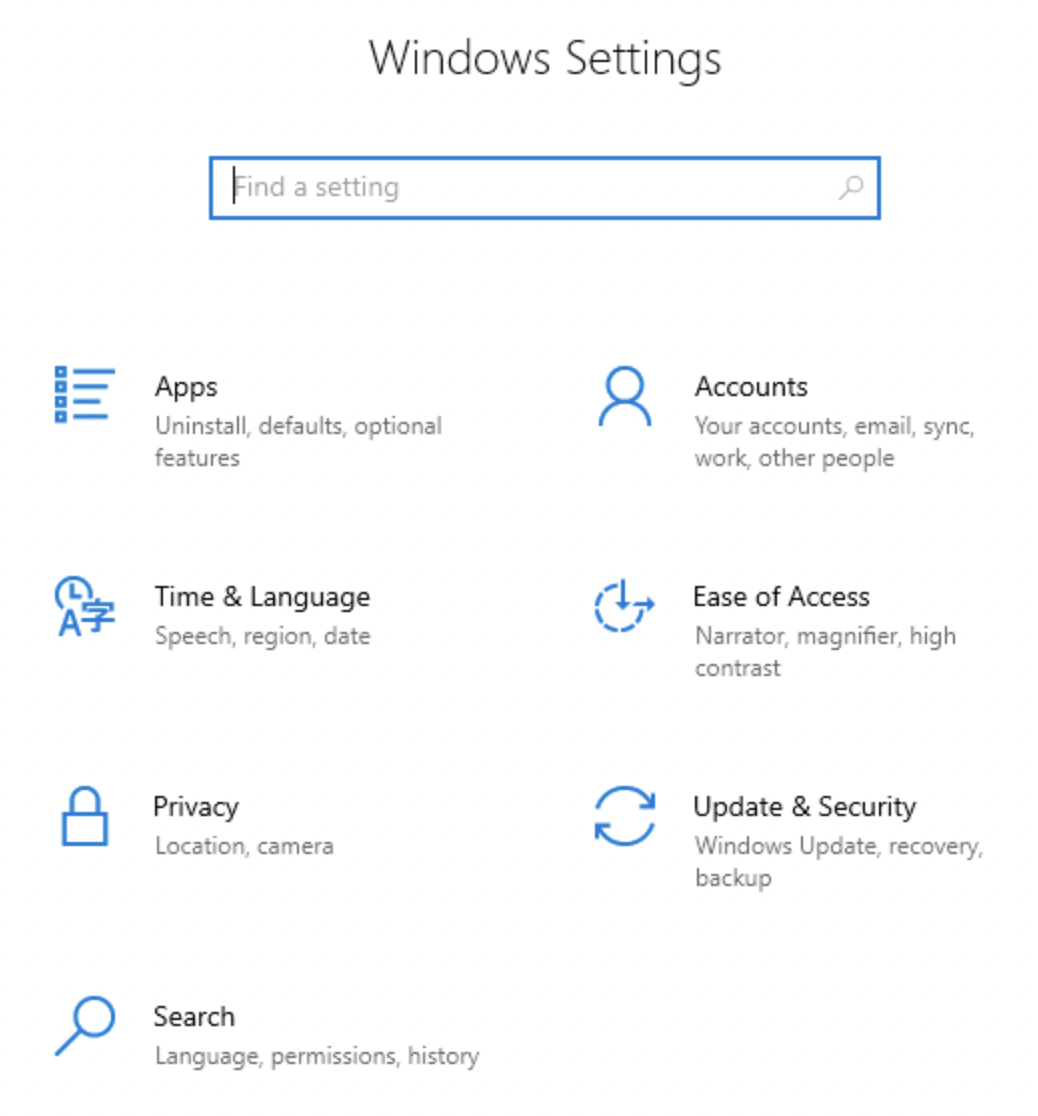
**Windows Updates**

Windows Update là 1 dịch vụ của Microsoft cung cấp các cập nhật bảo mật, nâng cấp tính năng và bản vá cho hệ điều hành cũng như các phần mềm của Microsoft như Microsoft Defender.

Các bản cập nhật được phát hành vào ngày 2 thứ ba của mỗi tháng. Không phải cứ thứ ba mới được cập nhật bản vá. Nếu cập nhật quan trọng, Microsoft sẽ đẩy bản update qua dịch vụ Windows Update để các thiết bị tự động cập nhật.

Windows Update nằm ở Settings.

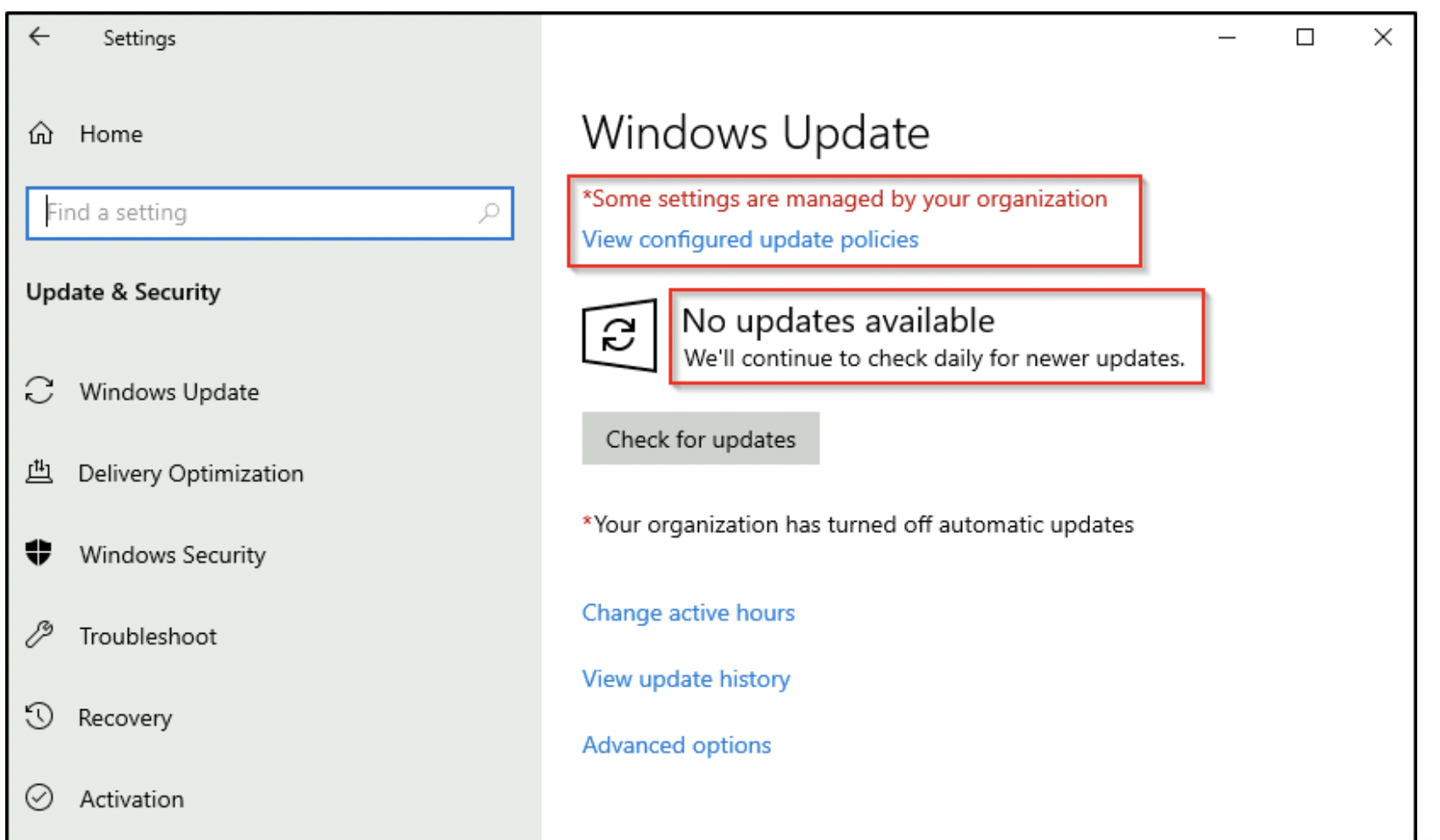
Một cách khác để truy cập các bản update của windows là chạy CMD, gõ lệnh control /name Microsoft.WindowsUpdate



Trong máy ảo, có một vài thứ cần nhấn mạnh:

Windows Update settings đang ‘managed’. (home users sẽ không thấy tin này)

Không có bản update nào cho máy ảo (máy ảo không có truy cập internet để giao tiếp với Microsoft nhận những bản cập nhật mới)

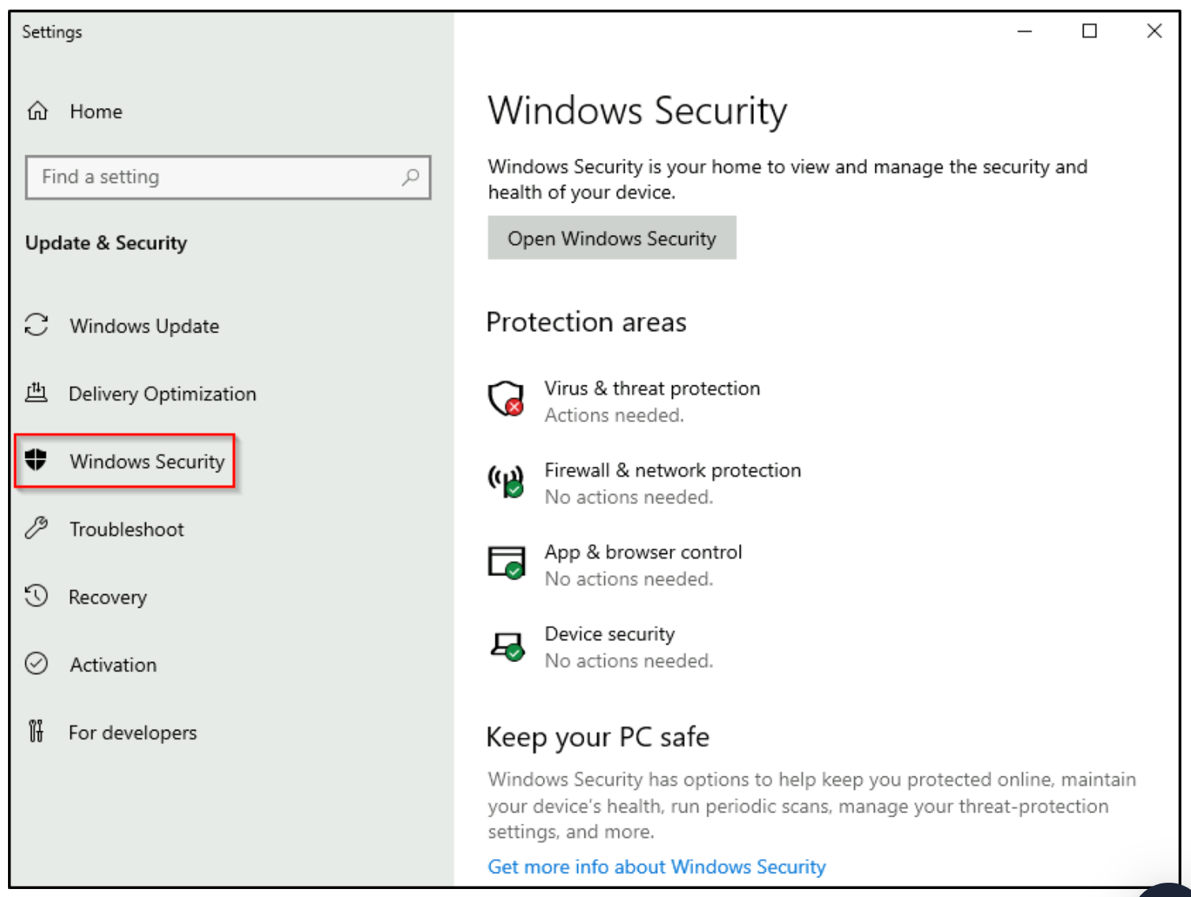


Qua nhiều năm, người dùng Windows đã quen với việc đẩy các bản cập nhật Windows sang một thời điểm muộn hơn hoặc không cập nhật hết. Rất nhiều lí do cho vấn đề này, một là phải khởi động lại sau bản cập nhật của Windows.

Microsoft đã chú ý giải quyết vấn đề này trong Win10. Các bản cập nhật không thể bị bỏ qua hoặc đẩy sang 1 trang khác đến khi quên. Các bản update có thể trì hoãn nhưng vẫn xảy ra và máy tính của bạn sẽ khởi động lại. Microsoft cung cấp các bản update này để giữ cho thiết bị an toàn và bảo mật.

**Windows Security**

Windows Security là ngôi nhà quản lý các công cụ bảo vệ thiết bị và dữ liệu của bạn.



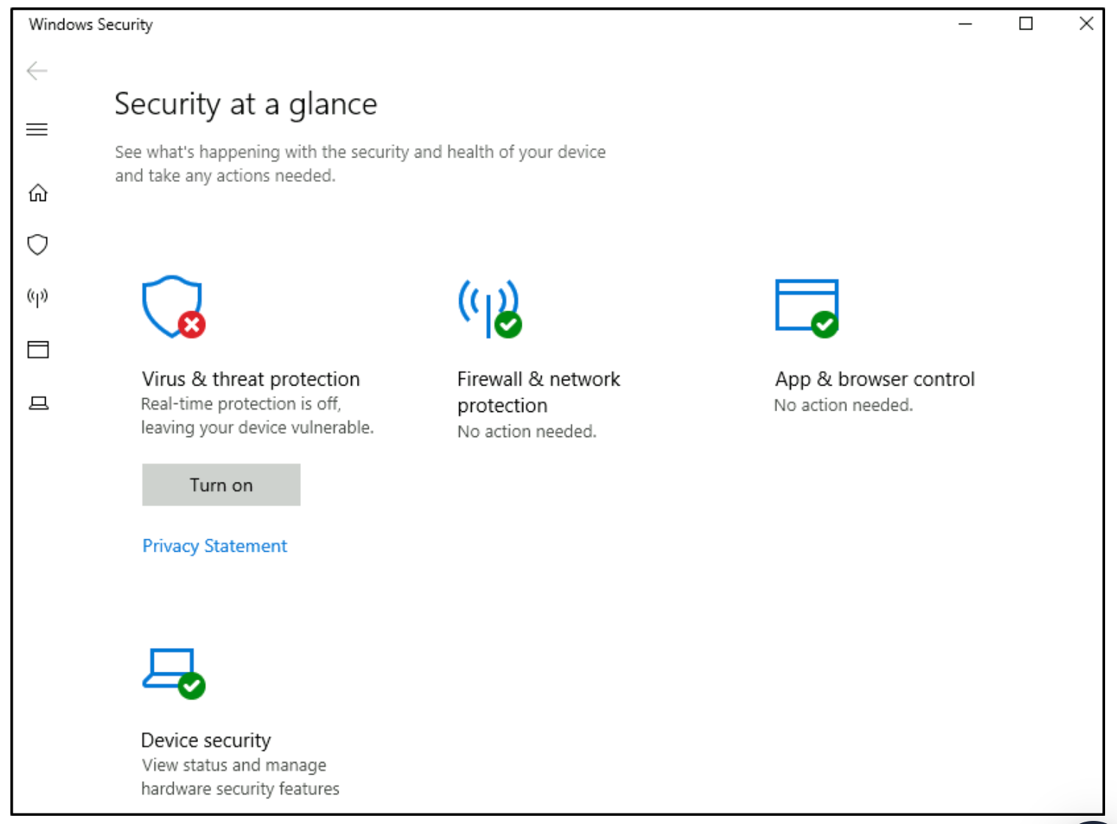
Để sự chú ý của bạn vào Protection areas:

* Virus & threat protection
* Firewall & network protection
* App & browser control
* Device security

Các icons trạng thái:

* Xanh nghĩa là thiết bị của bạn được bảo vệ đầy đủ, và không có bất kỳ hành động nào được đề xuất.
* Vàng nghĩa là 1 khuyến nghị an toàn để bạn xem xét
* Đỏ là lời cảnh báo có điều gì đó bạn cần chú ý ngay lập tức

Chọn Open Windows Security



**Virus & threat protection**

Nó được chia thành hai phần:

* Current threats
* Virus & threat protection settings

**Current threats**



**Scan options**

* Quick scan: kiểm tra các thư mục trong hệ thống của bạn nơi các mối đe dọa thường được tìm thấy
* Full scan: kiểm tra tất cả tập tin và chương trình đang chạy trên ổ đĩa cứng. Lần quét này có thể mất hơn 1 giờ.
* Custom scan: chọn tập tin và vị trí bạn kiểm tra

**Lịch sử threat**

* Last scan: Windows Defender Antivirus tự động quét thiết bị của bạn để tìm virus và các mối đe dọa khác.
* Quarantined threats: cô lập các mối đe dọa và ngăn chặn chúng chạy trên thiết bị. Chúng sẽ được loại bỏ định kỳ.
* Allow threats: là các mối đe dọa đã xác định, được bạn cho phép chạy trên thiết bị.

**Cảnh báo:** chỉ cho phép 1 item chạy khi bạn biết mình đang làm gì

**Virus & threat protection settings**



**Manage settings**

* Real-time protection: xác định và ngăn mã độc cài đặt và chạy trên thiết bị
* Cloud-delivered protection: cung cấp khả năng bảo vệ tăng cường và nhanh hơn nhờ truy cập dữ liệu bảo mật mới nhất trên cloud.
* Automatic sample submission: tự động gửi các file mẫu đến Microsoft để giúp bảo vệ bạn khỏi các mối đe dọa tiềm tàng
* Controlled folder access: bảo vệ các tập tin, thư mục, bộ nhớ trên thiết bị khỏi những thay đổi trái phép của ứng dụng xấu.
* Exclusions: Windows Defender Antivirus sẽ không quét các mục bạn đã loại trừ.
* Notifications: Windows Defender Antivirus sẽ gửi thông báo quan trọng về tình trạng và bảo mật của thiết bị.

Cảnh báo: những mục bị loại trừ có thể chứa mối đe dọa làm cho thiết bị bạn bị dính lỗ hổng. Chỉ dùng lựa chọn này khi bạn biết mình đang làm gì.

**Virus & threat protection updates**

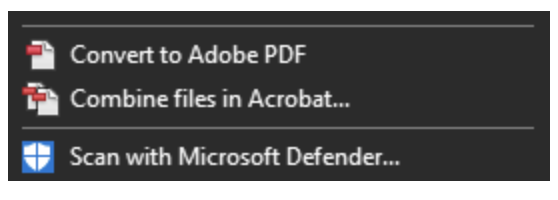
* Check for updates: kiểm tra các bản cập nhật bằng tay để nâng cấp Windows Defender Antivirus

**Ransomware protection**

* Controlled folder access: Ransomware protection yêu cầu tính năng này để thực thi do đó cũng phải bật Real-time protection

**Lưu ý:** Real-time production bị tắt trong máy ảo để giảm nguy cơ xảy ra các vấn đề về hiệu suất. Vì máy ảo không thể kết nối Internet và không có bất cứ mối đe dọa nào nên điều này là an toàn. Real-time protection nên được thực thi trong các thiết bị Windows cá nhân nếu bạn không có các phần mềm của bên thứ ba cung cấp lớp bảo vệ tương tự. Đảm bảo nó luôn cập nhật và thực thi.

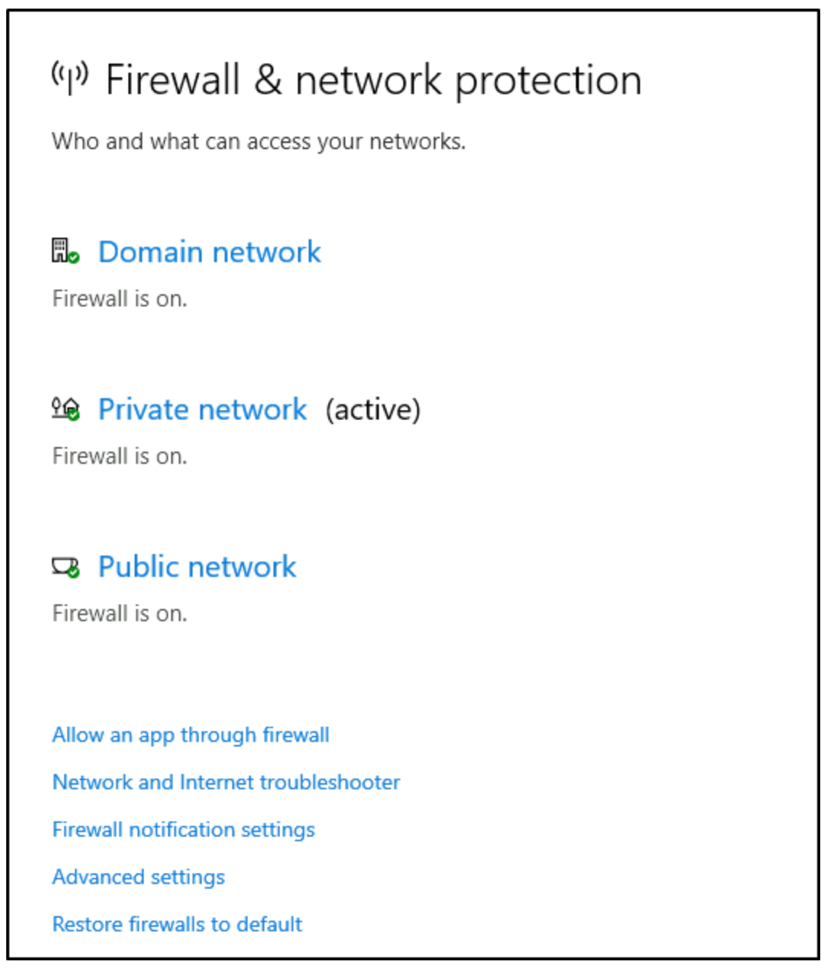
**Tip:** Bạn có thể thực hiện scan theo yêu cầu với bất kì thư mục hay tập tin nào bằng cách click chuột phải vào item và chọn “Scan with Microsoft Defender”.



**Firewall & network protection**

**Tường lửa là gì?**

Với Microsoft, lưu lượng vào và ra các thiết bị là cái chúng ta gọi là ports. Tường lửa là cái kiểm soát những gì được và quan trọng hơn là không được phép đi qua cổng đó. Bạn có thể nghĩ nó giống như 1 bảo vệ đứng trước cửa, kiểm tra ID của mọi thứ cố gắng đi vào hay thoát ra.



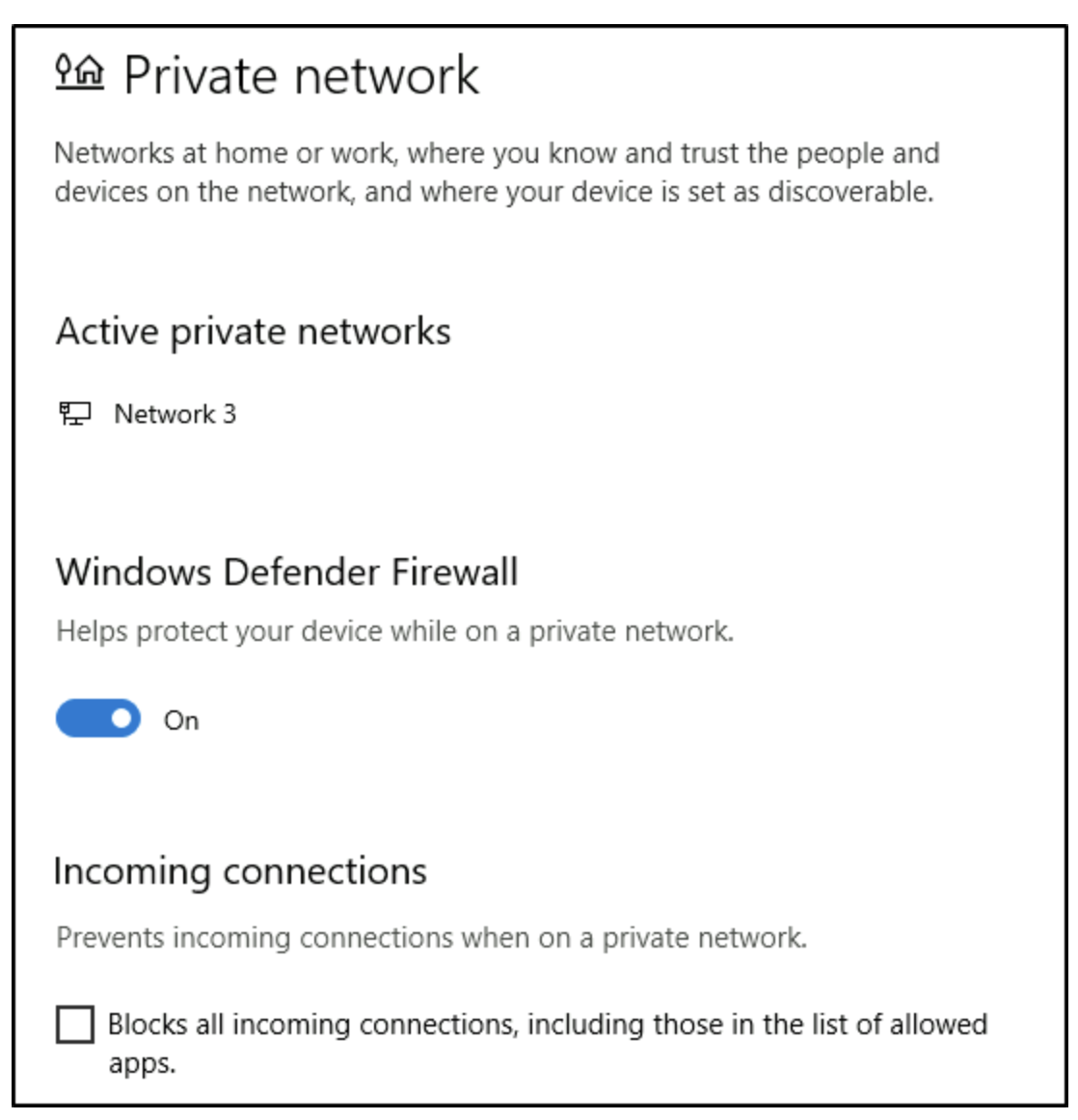
Mỗi mạng có các icon trạng thái khác nhau.

Sự khác nhau giữa 3 (Domain, Private và Public)?

Windows Firewall cung cấp 3 cấu hình tường lửa: domain, private và public.

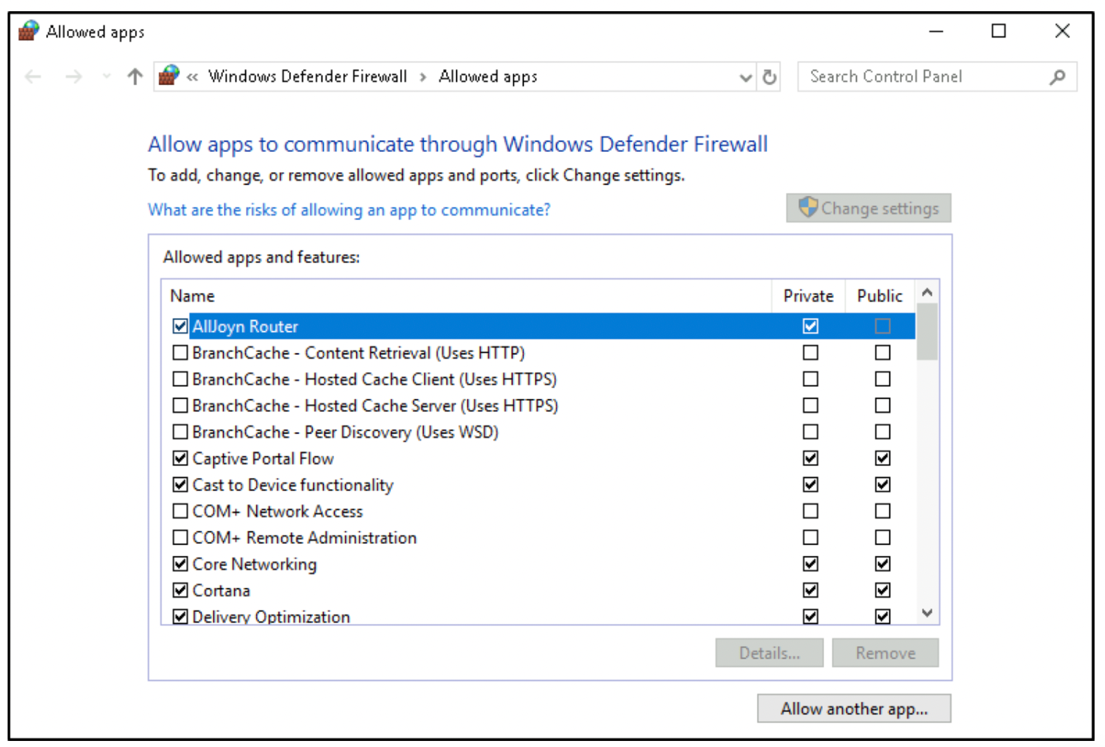
* Domain: cấu hình domain áp dụng cho các mạng mà hệ thống máy chủ có thể xác thực để lên domain controller.
* Private: cấu hình private là cấu hình do người dùng tự định nghĩa và chỉ định mạng riêng hoặc mạng gia đình.
* Public: cấu hình mặc định là cấu hình public, chỉ định các mạng chung như Wifi ở tiệm café, sân bay,…

Nếu bạn chọn bất cứ cấu hình tường lửa nào, 1 màn hình khác sẽ xuất hiện với hai lựa chọn: tắt/bật tường lửa và chặn tất cả kết nối đến.



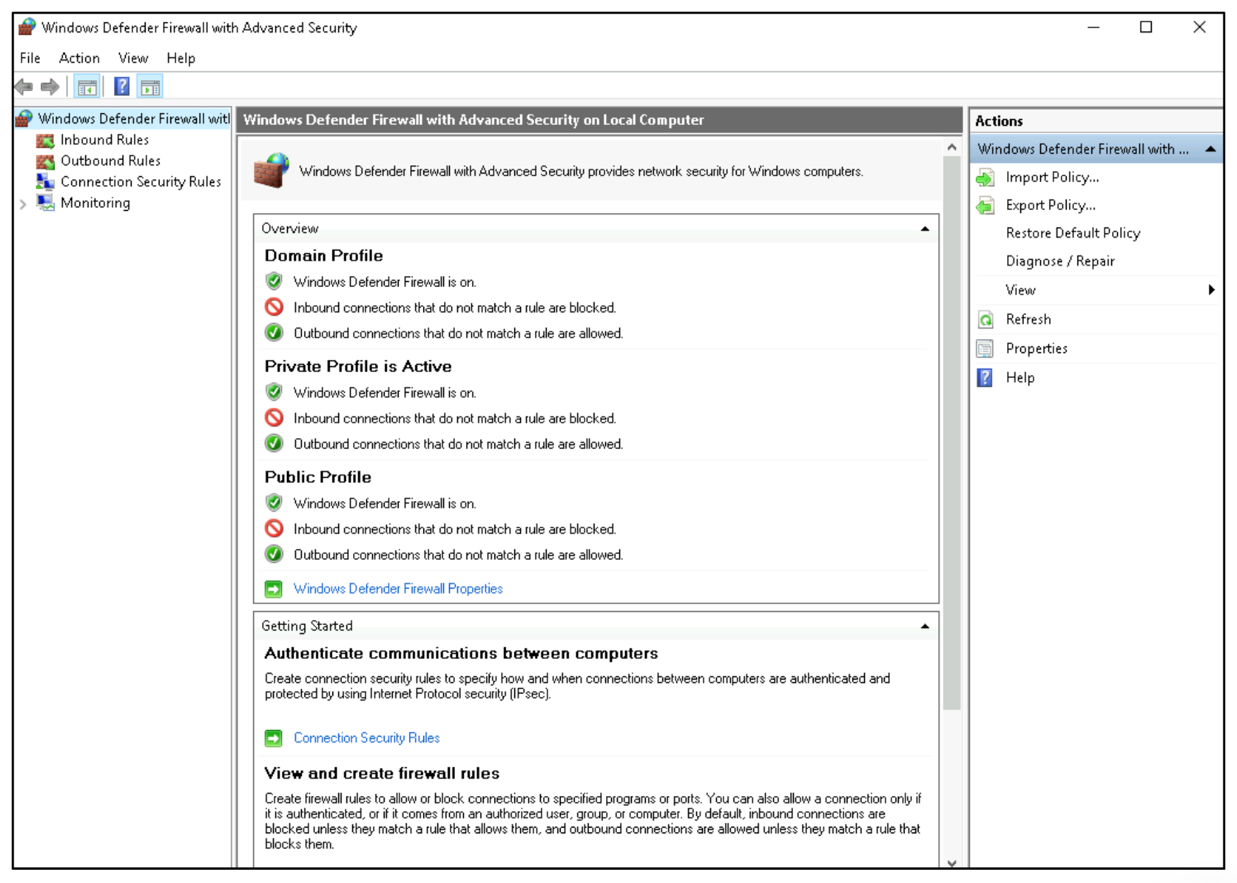
Cảnh báo: nếu bạn không tự tin 100% cái bạn đang làm, bạn nên bật Windows Defender Firewall.

**Cho phép 1 ứng dụng qua tường lửa:**



Bạn có thể xem các cài đặt mặc định của 1 cấu hình bất kỳ. Trong hình trên, một vài ứng dụng truy cập trong cấu hình Private hay Public của tường lửa. Một vài ứng dụng sẽ cung cấp thêm thông tin nếu nó khả thi ở nút Details.

**Advanced Settings**

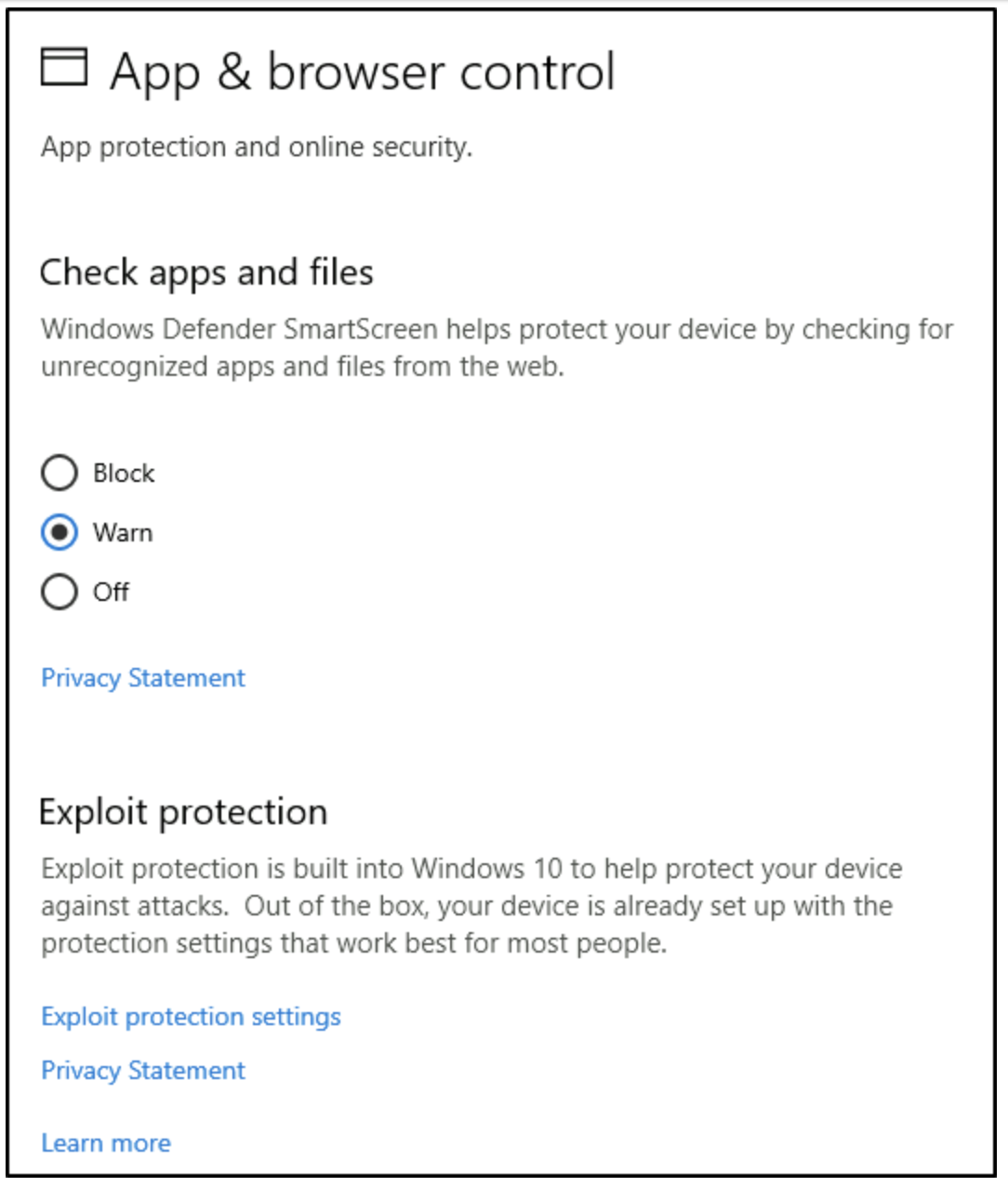


Việc cấu hình Windows Defender Firewall chỉ dành cho những người dùng nâng cao.

Lệnh để mở Windows Defender Firewall is WF.msc

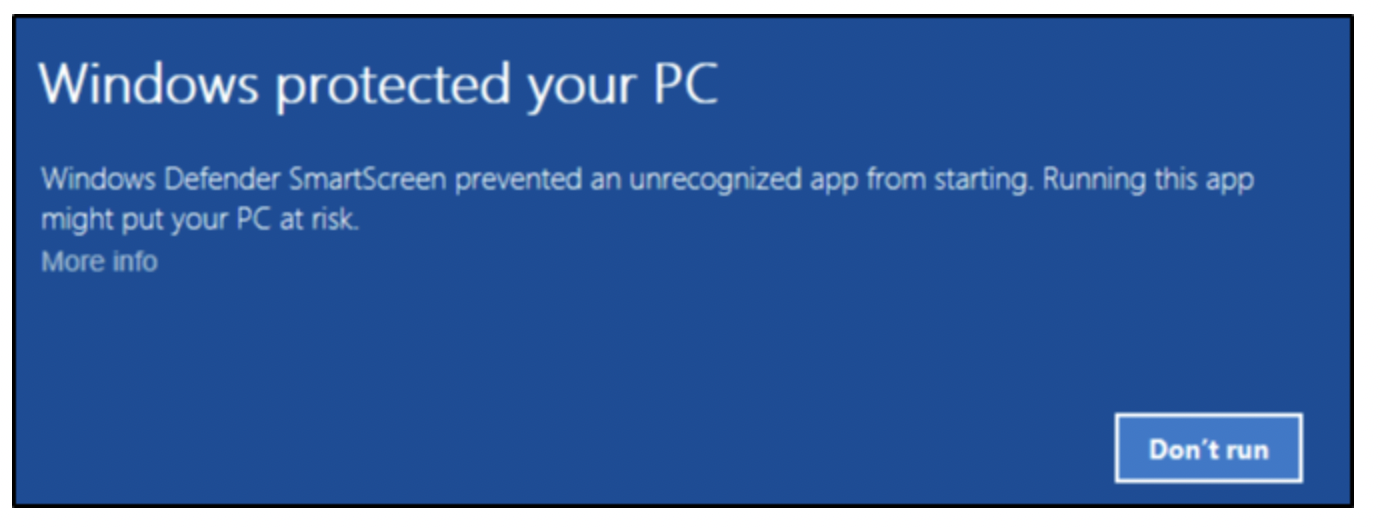
**App & browser control**

Microsoft Defender SmartScreen bảo vệ chống lại phishing hay các trang web/ứng dụng xấu và việc tải các tập tin độc hại.



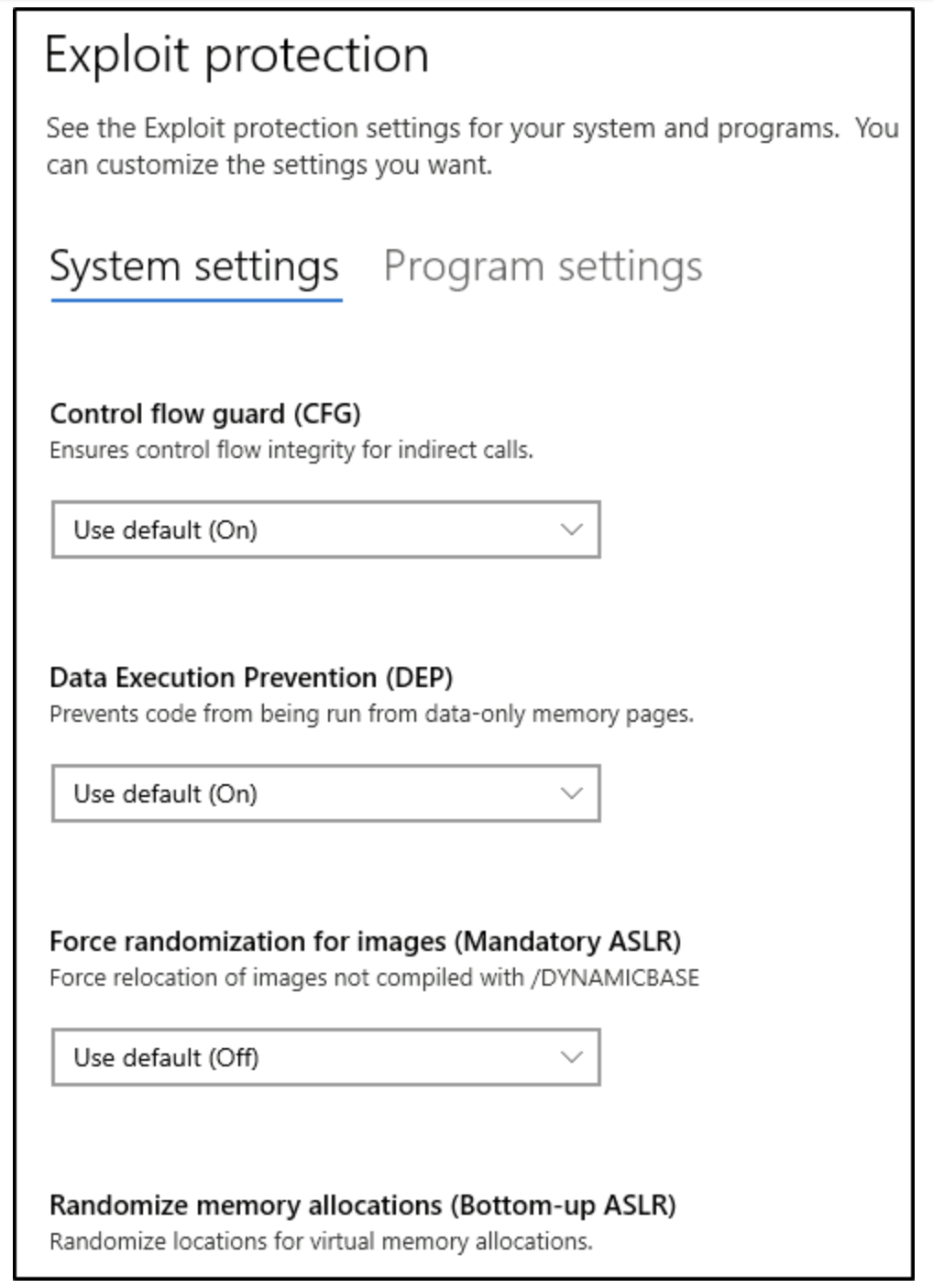
**Check apps and files**

* Windows Defender SmartScreen bảo vệ thiết bị của bạn bằng cách kiểm tra các ứng dụng và tập tin không được nhận dạng từ web.



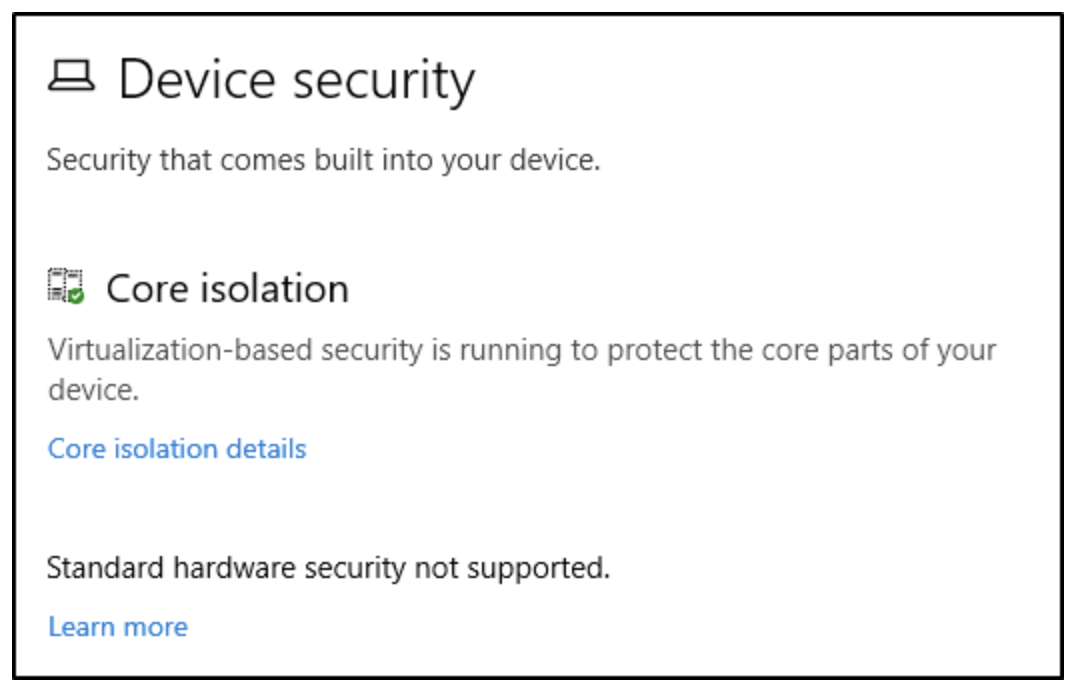
**Exploit protection**

* Exploit protection được dựng sẵn ở Windows 10 để giúp bảo vệ thiết bị của bạn khỏi các cuộc tấn công.



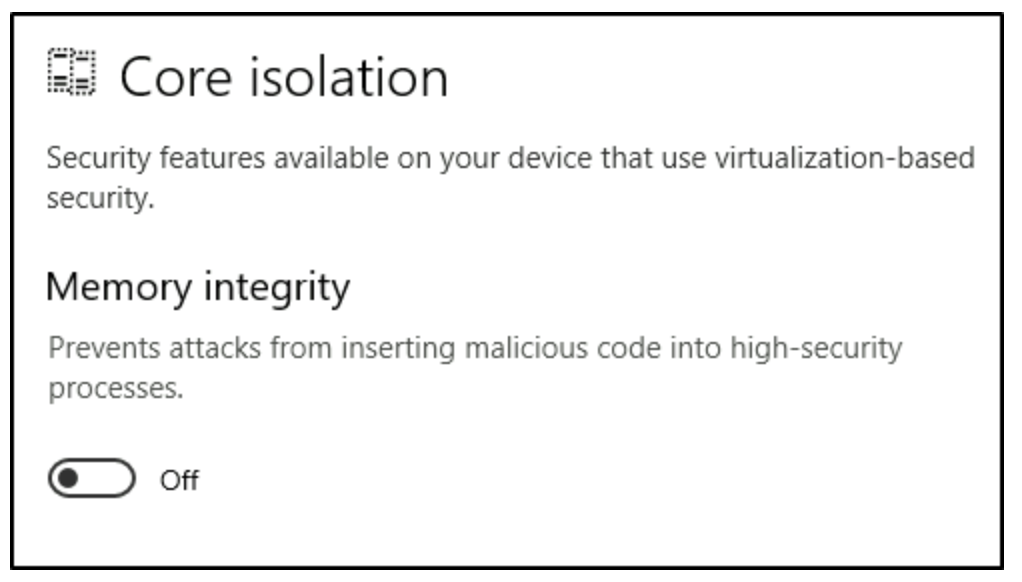
**Cảnh báo:** nếu bạn không biết mình nên làm gì, bạn nên để cài đặt mặc định.

**Device security**



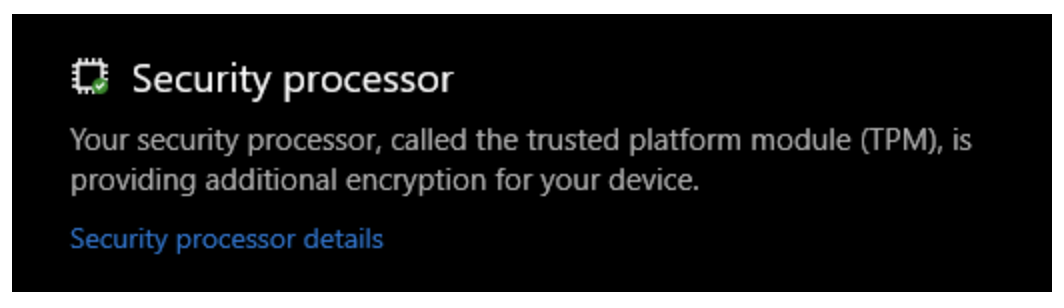
**Core Isolation**

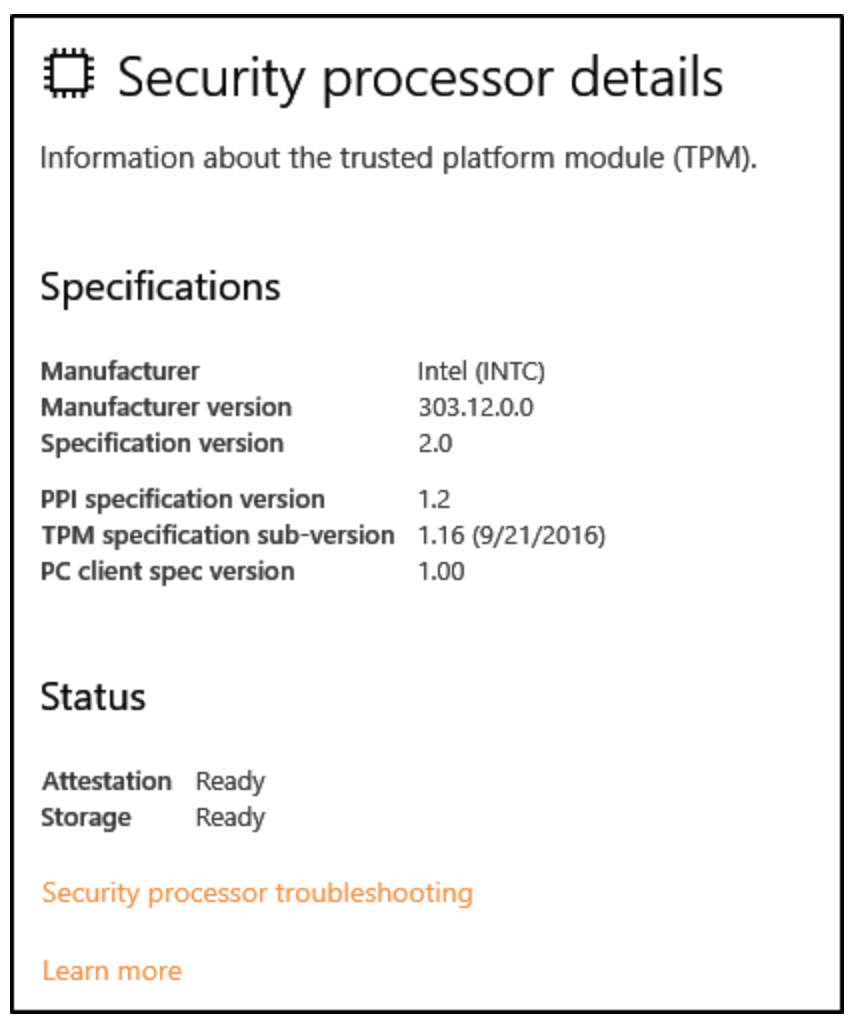
* Memory Integrity: ngăn chặn các cuộc tấn công tiêm mã độc vào trong tiến trình có tính bảo mật cao.



Hình dưới hiển thị 1 tính năng bảo mật khác trong Windows 10:

**Security processor**





**Trusted Platform Module (TPM) là gì?**

Trusted Platform Module (TPM) được thiết kế để cung cấp thêm chức năng liên quan đến bảo mật dựa trên phần cứng. TPM chip là 1 vi xử lí mật mã được thiết kế để thực hiện các hoạt động liên quan đến mã hóa. Chip bao gồm nhiều cơ chế bảo mật để chống giả mạo và phần mềm độc không thể can thiệp vào các chức năng bảo mật của TPM.

**BitLocker**

**BitLocker là gì?**

BitLocker Drive Encryption là 1 tính năng bảo vệ dữ liệu tích hợp với hệ điều hành và giải quyết các mối đe dọa về việc đánh cắp hoặc lộ dữ liệu từ các máy tính bị mất, đánh cắp hoặc ngừng hoạt động.

Trên các thiết bị đã cài đặt TPM, BitLocker cung cấp 1 lớp bảo vệ tốt nhất.

BitLocker cung cấp lớp bảo vệ tốt nhất khi được dùng với Trusted Platform Module phiên bản 1.2 hoặc sau đó nữa. TPM là 1 phần cứng đã được cài đặt trên nhiều máy tính mới. Nó làm việc với BitLocker để giúp bảo vệ dữ liệu người dùng, đảm bảo máy tính không bị can thiệp trong khi hệ thống ngưng hoạt động.

**Volume Shadow Copy Service**

Volume Shadow Copy Service (VSS) điều phối các hoạt động cần thiết để tạo consistent shadow copy (snapshot hay bản sao chép tại 1 thời điểm) của dữ liệu với mục đích là sao lưu.

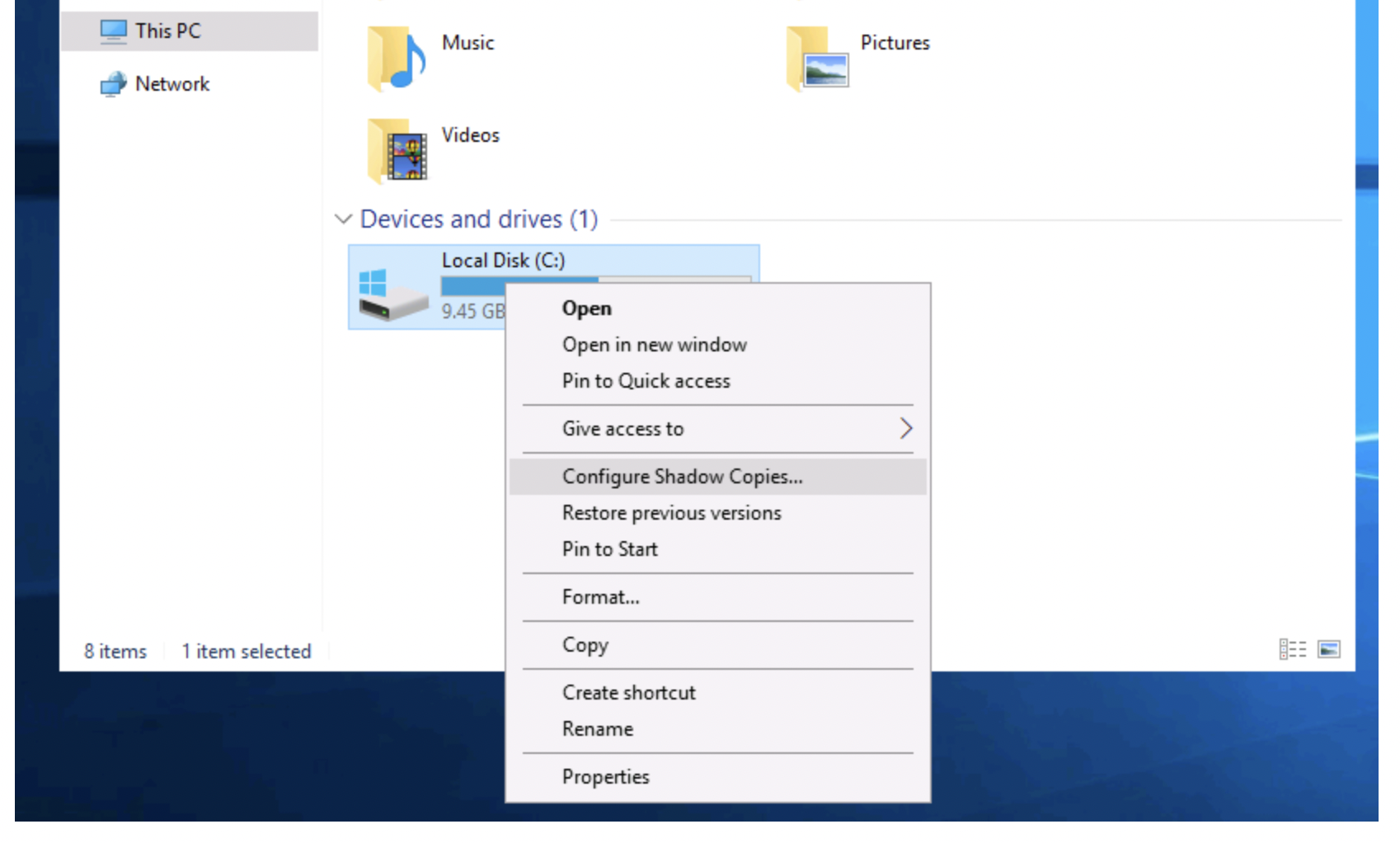
Volume Shadow Copies được lưu trữ trong thư mục System Volume Information trên mỗi drive đã được bật bảo vệ.

Nếu VSS được bật (System Protection được bật) bạn có thể thực hiện các tác vụ sau từ cài đặt hệ thống nâng cao:

* Tạo 1 điểm khôi phục
* Thực hiện khôi phục hệ thống
* Cấu hình các cài đặt khôi phục
* Xóa các điểm khôi phục

Từ khía cạnh bảo mật, những người viết mã độc biết tính năng này của Windows và viết mã để tìm kiếm các tập tin này để xóa chúng. Làm như vậy sẽ khiến bạn không thể khôi phục sau cuộc tấn công mã độc nếu bạn không có bản sao ngoại tuyến.

Nếu bạn muốn cấu hình Shadow Copies trong máy ảo, làm như sau:



Nếu bạn muốn tương tác trực tiếp với VSS, hãy khám phá Day23 của Advent of Cyber 2

