F-Secure Anti-Virus 2013

Nội dung

Chương 1: Cài đặt.....5

Trước khi bạn cài đặt lần đầu tiên.....6
Cài đặt sản phẩm lần đầu tiên.....6
Cài đặt và nâng cấp ứng dụng.....6
Trợ giúp và Hỗ trợ.....7

Chương 2: Bắt đầu.....9

Cách sử dụng bản cập nhật tự động.....10
- Kiểm tra trạng thái cập nhật.....10
- Thay đổi cài đặt kết nối Internet.....10
- Kiểm tra trạng thái của Mạng Bảo vệ trong Thời gian thực.....11

Cách xem các tác vụ sản phẩm đã thực hiện.....11
- Xem lịch sử thông báo.....11
- Thay đổi cài đặt thông báo.....11

Mạng Bảo vệ Thời gian thực.....12
- Mạng Bảo vệ Thời gian thực là gì.....12
- Các lợi ích của Mạng Bảo vệ Thời gian thực.....12
- Thông tin bạn đóng góp.....13
- Cách chúng tôi bảo vệ bảo mật của bạn.....14
- Trở thành người đóng góp cho Mạng Bảo vệ Thời gian thực.....14
- Câu hỏi về Mạng Bảo vệ Thời gian thực.....15

Làm thế nào để biết đăng ký của tôi không hợp lệ.....15
- Trung tâm hành động.....15
- Kích hoạt đăng ký.....16

Chương 3: Giới thiệu.....17

Xem toàn bộ trạng thái bảo vệ của tôi.....18
Xem thống kê sản phẩm.....18
Xử lý các bản cập nhật sản phẩm.....19
- Xem phiên bản cơ sở dữ liệu.....19
- Thay đổi cài đặt băng thông rộng di động.....19

Vi-rút và phần mềm độc hại khác là gì.....20
- Vi-rút.....20
- Phần mềm gián điệp.....20
- Rootkit.....21
- Phần mềm nguy hiểm.....21

Chương 4: Bảo vệ máy tính của bạn khỏi phần mềm độc hại.....23
Cách quét máy tính của tôi.....24
Quét tệp một cách tự động.....24
Quét tệp một cách thủ công.....26
Quét e-mail.....29
Xem kết quả quét.....30
Cách loại trừ tệp khỏi quá trình quét.....30
Loại trừ các loại tệp.....30
Loại trừ tệp theo vị trí.....31
Xem các ứng dụng được loại trừ.....31
Cách sử dụng khu vực cách ly.....32
Xem các mục được cách ly.....32
Khôi phục mục đã cách ly.....33
DeepGuard là gì.....33
Bật hoặc tắt DeepGuard.....34
Cho phép các ứng dụng mà DeepGuard đã chặn.....34
Sử dụng DeepGuard ở chế độ tương thích.....34
Tác vụ cần thực hiện với cảnh báo hành vi đáng ngờ.....35

Chương

1

Cài đặt

Chủ đề:

- *Trước khi bạn cài đặt lần đầu tiên*
- *Cài đặt sản phẩm lần đầu tiên*
- *Cài đặt và nâng cấp ứng dụng*
- *Trợ giúp và Hỗ trợ*

Trước khi bạn cài đặt lần đầu tiên

Cảm ơn bạn đã chọn F-Secure.

Để cài đặt sản phẩm, bạn cần những mục sau:

- CD cài đặt hoặc gói cài đặt. Nếu bạn đang sử dụng máy tính xách tay không có ổ CD, bạn có thể tải xuống gói cài đặt từ *www.f-secure.com/netbook*.
- Mã đăng ký của bạn.
- Kết nối Internet.

Nếu bạn có sản phẩm bảo mật từ nhà cung cấp khác, trình cài đặt sẽ cố xoá sản phẩm bảo mật đó một cách tự động. Nếu việc này không diễn ra, vui lòng xoá sản phẩm bảo mật đó một cách thủ công.

Ghi chú: Nếu bạn có nhiều tài khoản trên máy tính, hãy đăng nhập bằng đặc quyền của quản trị viên khi cài đặt.

Cài đặt sản phẩm lần đầu tiên

Hướng dẫn cài đặt sản phẩm.

Thực hiện theo các hướng dẫn sau để cài đặt sản phẩm.

1. Đưa đĩa CD vào hoặc bấm nhấp đúp vào trình cài đặt bạn đã tải xuống.

   Nếu đĩa CD không bắt đầu một cách tự động, hãy đi đến Windows Explorer, nhấp đúp vào biểu tượng CD-ROM và nhấp đúp vào tập tin cài đặt để bắt đầu quá trình cài đặt.

2. Làm theo các chỉ dẫn trên màn hình.

   - Nếu bạn đã mua sản phẩm này trên đĩa CD từ cửa hàng, bạn có thể tìm thấy mã đăng ký ở mặt sau của Hướng dẫn Cài đặt Nhanh.
   - Nếu bạn đã tải xuống sản phẩm từ F-Secure eStore, mã đăng ký được bao gồm trong e-mail xác nhận của đơn đặt hàng.

   Máy tính của bạn có thể cần phải khởi động lại trước khi xác thực đăng ký của bạn và tải xuống các cập nhật mới nhất từ Internet. Nếu bạn đang cài đặt từ đĩa CD, hãy nhớ lấy CD Cài đặt ra trước khi khởi động lại máy tính của bạn.

Cài đặt và nâng cấp ứng dụng

Các hướng dẫn kích hoạt đăng ký mới của bạn.

Làm theo các hướng dẫn sau để kích hoạt đăng ký mới của bạn hoặc để cài đặt ứng dụng mới bằng cách sử dụng bảng khởi chạy:

Ghi chú: Bạn có thể tìm thấy biểu tượng bảng khởi chạy trên khay hệ thống Windows.

1. Trên bảng khởi chạy, nhấp phải vào biểu tượng ngoài cùng bên phải.
   Trình đơn bật lên mở ra.
2. Chọn **Xem đăng ký của tôi**
3. Trong **Đăng ký của tôi**, hãy đi tới trang **Trạng thái đăng ký** và nhấp vào **Kích hoạt đăng ký**.
   Cửa sổ **Kích hoạt đăng ký** mở ra.

4. Nhập mã đăng ký của bạn cho ứng dụng và nhấp vào **OK**.
5. Sau khi đăng ký của bạn được xác thực và kích hoạt, hãy nhấp vào **Đóng**.
6. Trong **Đăng ký của tôi**, hãy đi tới trang **Trạng thái cài đặt**. Nếu quá trình cài đặt không bắt đầu tự động, hãy làm theo các hướng dẫn sau:
   a) Nhấp vào **Cài đặt**.
   Cửa sổ cài đặt mở ra.
   b) Nhấp **Tiếp theo**.
   Ứng dụng được tải xuống và quá trình cài đặt bắt đầu.
   c) Khi quá trình cài đặt hoàn tất, nhấp vào **Đóng**.

Đăng ký mới đã được kích hoạt.

Trợ giúp và Hỗ trợ

Bạn có thể truy cập phần trợ giúp sản phẩm trực tuyến bằng cách nhấp vào biểu tượng Trợ giúp hoặc bằng cách bấm F1 trong bất kỳ bàn hình nào của sản phẩm.

Sau khi bạn đăng ký giấy phép của mình, bạn có quyền sử dụng các dịch vụ bổ sung như các cập nhật sản phẩm và hỗ trợ sản phẩm miễn phí. Bạn có thể đăng ký tại *www.f-secure.com/register*.

Chương

2

Bắt đầu

Chủ đề:

- *Cách sử dụng bản cập nhật tự động*
- *Cách xem các tác vụ sản phẩm đã thực hiện*
- *Mạng Bảo vệ Thời gian thực*
- *Làm thế nào để biết đăng ký của tôi không hợp lệ*

Thông tin về cách bắt đầu sử dụng sản phẩm

Phần này mô tả cách thay đổi cài đặt chung và quản lý đăng ký của bạn qua bảng khởi chạy.

Cài đặt chung của bảng khởi chạy là những cài đặt áp dụng cho tất cả các chương trình đã được cài đặt trên bảng khởi chạy. Thay vì thay đổi cài đặt một cách riêng rẽ trong mỗi chương trình thì bạn có thể chỉ cần chỉnh sửa cài đặt chung. Sau đó, cài đặt chung này được các chương trình đã cài đặt sử dụng.

Cài đặt chung của bảng khởi chạy bao gồm:

- Tải xuống, nơi bạn có thể xem thông tin về những cập nhật đã được tải xuống và kiểm tra một cách thủ công nếu cập nhật mới sẵn có.
- Cài đặt kết nối, nơi bạn có thể thay đổi cách máy tính của mình kết nối với Internet.
- Thông báo, nơi bạn có thể xem thông tin trước đây và đặt loại thông báo mà bạn muốn xem.
- Cài đặt bảo mật, nơi bạn có thể chọn liệu máy tính của mình có được phép kết nối với Mạng Bảo vệ Thời gian thực hay không.

Bạn cũng có thể quản lý đăng ký của mình cho những chương trình đã được cài đặt qua bảng khởi chạy.

Cách sử dụng bản cập nhật tự động

Bản cập nhật tự động giúp tính năng bảo vệ trên máy tính của bạn luôn cập nhật.

Sản phẩm sẽ truy lục bản cập nhật mới nhất cho máy tính của bạn khi bạn kết nối với Internet. Nó phát hiện lưu lượng truy cập mạng và không làm ảnh hưởng đến việc sử dụng Internet khác ngay cả với kết nối mạng chậm.

Kiểm tra trạng thái cập nhật

Xem ngày và giờ của cập nhật mới nhất.

Khi cập nhật tự động được bật, sản phẩm sẽ tự động nhận được các cập nhật mới nhất khi bạn kết nối với Internet.

Để đảm bảo rằng bạn có các cập nhật mới nhất:

1. Trên bảng khởi chạy, nhấp phải vào biểu tượng ngoài cùng bên phải.
   Trình đơn bật lên xuất hiện.
2. Chọn **Mở cài đặt chung**.
3. Chọn **Cập nhật tự động** > **Tải xuống**.
4. Nhấp vào **Kiểm tra ngay bây giờ**.
   Sản phẩm kết nối với Internet và kiểm tra các cập nhật mới nhất. Nếu tính năng bảo vệ không cập nhật, sản phẩm sẽ truy lục các cập nhật mới nhất.

   Ghi chú: Nếu bạn đang sử dụng modem hoặc có kết nối ISDN với Internet, kết nối phải hoạt động để kiểm tra các cập nhật.

Thay đổi cài đặt kết nối Internet

Thông thường, không cần thiết phải thay đổi cài đặt mặc định, nhưng bạn có thể định cấu hình cách máy chủ kết nối với Internet để có thể tự động nhận được các cập nhật.

Để thay đổi cài đặt kết nối Internet:

1. Trên bảng khởi chạy, nhấp phải vào biểu tượng ngoài cùng bên phải.
   Trình đơn bật lên xuất hiện.
2. Chọn **Mở cài đặt chung**.
3. Chọn **Cập nhật tự động** > **Kết nối**.
4. Trên danh sách **Kết nối Internet**, chọn cách máy tính của bạn được kết nối với Internet.
   - Chọn **Giả sử luôn kết nối** nếu bạn có kết nối mạng vĩnh viễn.

     Ghi chú: Nếu thực tế máy tính của bạn không có kết nối mạng vĩnh viễn và được thiết lập quay số theo yêu cầu, việc chọn **Giả sử luôn kết nối** có thể dẫn đến nhiều quay số.
   - Chọn **Phát hiện kết nối** để chỉ tìm kiếm các cập nhật khi sản phẩm phát hiện kết nối mạng đang hoạt động.
   - Chọn **Phát hiện lưu lượng truy cập** để chỉ tìm kiếm các cập nhật khi sản phẩm phát hiện lưu lượng truy cập mạng khác.

     Mẹo: Nếu bạn có cấu hình phần cứng bất thường khiến cài đặt **Phát hiện kết nối** phát hiện kết nối mạng đang hoạt động ngay cả khi không có, hãy chọn **Phát hiện lưu lượng truy cập** thay thế.

5. Trên danh sách **Proxy HTT**, chọn xem máy tính của bạn có đang sử dụng *máy chủ proxy* để kết nối với Internet hay không.
   - Chọn **Không có Proxy HTTP** nếu máy tính của bạn được kết nối trực tiếp với Internet.
   - Chọn **Định cấu hình proxy HTTP theo cách thủ công** để định cấu hình cài đặt *proxy HTTP*.
   - Chọn **Sử dụng proxy HTTP của trình duyệt của tôi** để sử dụng cùng một cài đặt *proxy HTTP* mà bạn đã định cấu hình trong trình duyệt web của mình.

Kiểm tra trạng thái của Mạng Bảo vệ trong Thời gian thực

Để hoạt động chính xác, nhiều tính năng của sản phẩm phụ thuộc vào kết nối Mạng Bảo vệ trong Thời gian thực.

Nếu có sự cố về mạng hoặc nếu tường lửa của bạn chặn lưu lượng truy cập Mạng Bảo vệ trong Thời gian thực, trạng thái sẽ là 'ngắt kết nối'. Nếu không có tính năng sản phẩm đã cài đặt nào yêu cầu truy cập vào Mạng Bảo vệ trong Thời gian thực, trạng thái sẽ là 'không sử dụng'.

Để kiểm tra trạng thái:

1. Trên bảng khởi chạy, nhấp phải vào biểu tượng ngoài cùng bên phải.
   Trình đơn bật lên xuất hiện.
2. Chọn **Mở cài đặt chung**.
3. Chọn **Cập nhật tự động** > **Kết nối**.

Trong **Mạng Bảo vệ trong Thời gian thực**, bạn có thể thấy trạng thái hiện tại của Mạng Bảo vệ trong Thời gian thực.

Cách xem các tác vụ sản phẩm đã thực hiện

Bạn có thể xem những tác vụ mà sản phẩm đã thực hiện nhằm bảo vệ máy tính của mình trên trang **Thông báo**.

Sản phẩm này sẽ hiển thị thông báo khi sản phẩm thực hiện tác vụ, chẳng hạn như khi sản phẩm tìm thấy vi-rút mà nó chặn. Nhà cung cấp dịch vụ của bạn cũng có thể gửi một số thông báo, chẳng hạn như để cho bạn biết về những dịch vụ mới sẵn có.

Xem lịch sử thông báo

Bạn có thể thấy những thông báo nào được hiển thị trong lịch sử thông báo

Để xem lịch sử thông báo:

1. Trên bảng khởi chạy, nhấp phải vào biểu tượng ngoài cùng bên phải.
   Trình đơn bật lên xuất hiện.
2. Chọn **Mở cài đặt chung**.
3. Chọn **Cài đặt khác** > **Thông báo**.
4. Nhấp vào **Hiển thị lịch sử thông báo**.
   Danh sách lịch sử thông báo mở.

Thay đổi cài đặt thông báo

Bạn có thể chọn loại thông báo mà bạn muốn sản phẩm hiển thị.

Để thay đổi cài đặt thông báo:

1. Trên bảng khởi chạy, nhấp phải vào biểu tượng ngoài cùng bên phải.
   Trình đơn bật lên xuất hiện.
2. Chọn **Mở cài đặt chung**.
3. Chọn **Cài đặt khác** > **Thông báo**.
4. Chọn hoặc bỏ chọn **Cho phép thông báo chương trình** để bật hoặc tắt thông báo chương trình.
   Khi cài đặt này được bật, sản phẩm sẽ hiển thị thông báo từ chương trình đã được cài đặt.
5. Chọn hoặc bỏ chọn **Cho phép thông báo khuyến mãi** để bật hoặc tắt thông báo khuyến mãi.
6. Nhấp vào **OK**.

Mạng Bảo vệ Thời gian thực

Tài liệu này mô tả Mạng Bảo vệ Thời gian thực, một dịch vụ trực tuyến từ F-Secure Corporation giúp xác định các ứng dụng và trang web sạch trong khi đưa ra sự bảo vệ chống lại phần mềm độc hại và các khai thác trang web.

Mạng Bảo vệ Thời gian thực là gì

Mạng Bảo vệ Thời gian thực là một dịch vụ trực tuyến đưa ra phản hồi nhanh chóng chống lại các mối đe doạ mới nhất dựa trên Internet.

Với tư cách là người đóng góp cho Mạng Bảo vệ Thời gian thực, bạn có thể giúp chúng tôi tăng cường sự bảo vệ chống lại các mối đe doạ mới và đang phát triển. Mạng Bảo vệ Thời gian thực thu thập số liệu thống kê của các ứng dụng không xác định, độc hại hoặc đáng ngờ nhất định và những việc mà các ứng dụng này thực hiện trên thiết bị của bạn. Thông tin này là ẩn danh và được gửi đến F-Secure Corporation để phân tích dữ liệu tổng hợp. Chúng tôi sử dụng thông tin được phân tích để cải tiến tính bảo mật trên thiết bị của bạn chống lại các mối đe doạ mới nhất và các tệp độc hại.

Mạng Bảo vệ Thời gian thực hoạt động như thế nào

Với tư cách là người đóng góp cho Mạng Bảo vệ Thời gian thực, bạn có thể cung cấp thông tin về các ứng dụng và trang web chưa biết, cũng như những ứng dụng độc hại và công cụ khai thác trên trang web. Mạng Bảo vệ Thời gian thực không theo dõi hoạt động của bạn trên web hoặc thu thập thông tin về trang web đã được phân tích, đồng thời không thu thập thông tin về các ứng dụng không bị nhiễm vi-rút được cài đặt trên máy tính của bạn.

Nếu bạn không muốn đóng góp dữ liệu này, Mạng Bảo vệ Thời gian thực sẽ không thu thập thông tin về các ứng dụng đã cài đặt hoặc các trang web đã truy cập. Tuy nhiên, sản phẩm cần truy vấn các máy chủ F-Secure đối với danh tiếng của các ứng dụng, trang web, tin nhắn và các đối tượng khác. Truy vấn được thực hiện bằng cách tổng kiểm tra mật mã hoá mà chính đối tượng được truy vấn không được gửi đến F-Secure. Chúng tôi không theo dõi dữ liệu mỗi một người dùng; chỉ bộ đếm truy cập của tệp hoặc trang web được gia tăng.

Không thể dừng hoàn toàn tất cả lưu lượng truy cập mạng đến Mạng Bảo vệ Thời gian thực do đây là phần bảo vệ được tích hợp do sản phẩm cung cấp.

Các lợi ích của Mạng Bảo vệ Thời gian thực

Với Mạng Bảo vệ Thời gian thực, bạn sẽ nhận được sự bảo vệ nhanh hơn và chính xác hơn chống lại các mối đe doạ mới nhất và bạn sẽ không phải nhận các cảnh báo không cần thiết về các ứng dụng đáng ngờ không độc hại.

Với tư cách là người đóng góp cho Mạng Bảo vệ Thời gian thực, bạn có thể giúp chúng tôi tìm ra những phần mềm độc hại mới và chưa bị phát hiện, cũng như xoá bỏ những cảnh báo nhầm có thể có trong cơ sở dữ liệu về định nghĩa vi-rút của chúng tôi.

Tất cả những người tham gia trong Mạng Bảo vệ Thời gian thực giúp đỡ lẫn nhau. Khi Mạng Bảo vệ Thời gian thực tìm thấy ứng dụng đáng ngờ trên thiết bị của bạn, bạn hưởng lợi từ các kết quả phân tích khi ứng dụng tương tự hiện đã được tìm thấy trên các thiết bị khác. Mạng Bảo vệ Thời gian thực nâng cao hiệu suất chung của thiết bị của bạn do sản phẩm bảo mật đã cài đặt không cần quét lại các ứng dụng mà Mạng Bảo vệ Thời gian thực đã phân tích và nhận thấy là sạch. Tương tự, thông tin về các trang web độc hại và tin nhắn hàng loạt không được yêu cầu được chia sẻ qua Mạng Bảo vệ Thời gian thực và chúng tôi có thể cung cấp cho bạn sự bảo vệ chính xác hơn chống lại các khai thác trang web và tin nhắn rác.

Càng có nhiều người đóng góp cho Mạng Bảo vệ Thời gian thực, thì mỗi người tham gia càng được bảo vệ tốt hơn.

Thông tin bạn đóng góp

Với tư cách là nhà đóng góp cho Mạng Bảo vệ Thời gian thực, bạn cung cấp thông tin về các ứng dụng được lưu trữ trên thiết bị của mình và các trang web bạn truy cập để Mạng Bảo vệ Thời gian thực có thể đưa ra sự bảo vệ chống lại các ứng dụng độc hại mới nhất và các trang web đáng ngờ.

Phân tích danh tiếng tệp

Mạng Bảo vệ Thời gian thực chỉ thu thập thông tin về các ứng dụng không có danh tiếng được xác định và các tệp đáng ngờ hoặc được xác định là phần mềm độc hại.

Mạng Bảo vệ Thời gian thực thu thập thông tin ẩn danh về các ứng dụng khả nghi và ứng dụng không bị nhiễm vi-rút trên thiết bị của bạn. Mạng Bảo vệ Thời gian thực chỉ thu thập thông tin về các tệp thực thi (như tệp Thực thi Di động trên nền tảng Windows, có phần mở rộng.cpl, .exe, .dll, .ocx, .sys, .scr, và .drv).

Thông tin được thu thập bao gồm:

- đường dẫn tệp của ứng dụng trong thiết bị của bạn,
- kích thước tệp và thời điểm tệp được tạo hoặc sửa đổi,
- thuộc tính của tệp và đặc quyền,
- thông tin chữ ký của tệp,
- phiên bản hiện tại của tệp và công ty đã tạo tệp đó,
- gốc tệp hoặc URL tải xuống của tệp, và
- F-Secure DeepGuard và kết quả phân tích diệt vi-rút của các tệp đã quét, và
- thông tin tương tự khác.

Mạng Bảo vệ Thời gian thực không bao giờ thu thập bất kỳ thông tin nào về tài liệu cá nhân của bạn, trừ khi chúng bị phát hiện là nhiễm vi-rút. Đối với mọi loại tệp độc hại, dịch vụ sẽ thu thập tên của vi-rút lây nhiễm và trạng thái khử nhiễm của tệp.

Với Mạng Bảo vệ Thời gian thực, bạn cũng có thể gửi các ứng dụng đáng ngờ để phân tích. Ứng dụng bạn gửi chỉ bao gồm các tệp Có thể thi hành trên Điện thoại di động. Mạng Bảo vệ Thời gian thực không bao giờ thu thập bất kỳ thông tin nào về tài liệu cá nhân của bạn và chúng không bao giờ được tự động tải lên để phân tích.

Gửi tệp để phân tích

Với Mạng Bảo vệ Thời gian thực, bạn cũng có thể gửi các ứng dụng đáng ngờ để phân tích.

Bạn có thể gửi ứng dụng đáng ngờ riêng lẻ một cách thủ công khi sản phẩm nhắc bạn làm như vậy. Bạn chỉ có thể gửi các tệp Có thể thi hành trên Điện thoại di động. Mạng Bảo vệ Thời gian thực không bao giờ tải lên các tài liệu cá nhân của bạn.

Phân tích danh tiếng trang web

Mạng Bảo vệ Thời gian thực không theo dõi hoạt động web của bạn hay thu thập thông tin về các trang web bạn hiện đã phân tích. Điều này đảm bảo rằng các trang web đã truy cập là an toàn khi bạn duyệt qua web.

Khi bạn truy cập trang web, Mạng Bảo vệ Thời gian thực kiểm tra tính an toàn của trang web đó và thông báo cho bạn nếu trang web bị đánh giá là đáng ngờ hoặc gây hại.

Nếu trang web bạn truy cập chứa nội dung độc hại hoặc đáng ngờ hoặc khai thái được xác định, Mạng Bảo vệ Thời gian thực thu thập toàn bộ URL của trang web để có thể phân tích nội dung trang web.

Nếu bạn truy cập trang web chưa được đánh giá, Mạng Bảo vệ Thời gian thực thu thập các tên miền và tên miền phụ, và trong một số trường hợp là đường dẫn đến trang web đã truy cập, để có thể phân tích và đánh giá trang web. Tất cả các tham số URL có thể chứa thông tin có thể được liên kết đến bạn theo định dạng có thể nhận dạng cá nhân bị xoá nhằm bảo vệ bảo mật của bạn.

Ghi chú: Mạng Bảo vệ Thời gian thực không đánh giá hay phân tích các trang web trong mạng cá nhân, do đó Mạng Bảo vệ Thời gian thực không bao giờ thu thập bất kỳ thông tin nào về địa chỉ IP mạng cá nhân của bạn (ví dụ: mạng nội bộ công ty).

Phân tích thông tin hệ thống

Mạng Bảo vệ Thời gian thực thu thập tên và phiên bản của hệ điều hành của bạn, thông tin về kết nối Internet và các thống kê sử dụng Mạng Bảo vệ Thời gian thực (ví dụ: số lần danh tiếng trang web được truy vấn và thời gian trung bình để trả lại kết quả cho truy vấn) để chúng tôi có thể giám sát và cải tiến dịch vụ.

Cách chúng tôi bảo vệ bảo mật của bạn

Chúng tôi truyền thông tin một cách bảo mật và tự động xoá bất kỳ thông tin cá nhân nào mà dữ liệu có thể chứa.

Mạng Bảo vệ Thời gian thực xoá dữ liệu nhận dạng trước khi gửi đến F-Secure và mã hoá tất cả thông tin được thu thập trong quá trình truyền để bảo vệ dữ liệu không bị truy cập trái phép. Thông tin được thu thập sẽ không bị xử lý riêng rẽ; chúng được tập hợp lại cùng với thông tin từ những cộng tác viên khác từ Mạng Bảo vệ Thời gian thực. Tất cả các dữ liệu được phân tích bằng phương pháp thống kê và ẩn danh, điều đó có nghĩa là không có dữ liệu nào được liên hệ tới bạn theo bất kỳ cách nào.

Bất kỳ thông tin nào có thể nhận dạng bạn một cách cá nhân sẽ không được đưa vào dữ liệu được thu thập. Mạng Bảo vệ Thời gian thực không thu thập các địa chỉ IP cá nhân hay thông tin cá nhân của bạn, chẳng hạn như các địa chỉ e-mail, tên người dùng và mật khẩu. Trong khi chúng tôi thực hiện mọi nỗ lực để xoá tất cả các dữ liệu có thể nhận dạng cá nhân, có thể một số dữ liệu nhận dạng vẫn còn trong thông tin được thu thập. Trong những trường hợp này, chúng tôi sẽ không tìm cách sử dụng dữ liệu được thu thập không có chủ ý này để nhận dạng bạn.

Chúng tôi áp dụng các biện pháp bảo mật nghiêm ngặt và các biện pháp bảo vệ vật lý, quản trị và kỹ thuật để bảo vệ dữ liệu được thu thập khi dữ liệu đó được truyền, lưu trữ và xử lý. Thông tin được lưu trữ ở các địa điểm an toàn và trên các máy chủ được chúng tôi kiểm soát, được đặt trong các văn phòng của chúng tôi hoặc tại văn phòng của nhà thầu phụ của chúng tôi. Chỉ những nhân viên có thẩm quyền mới được phép truy cập thông tin được thu thập.

F-Secure có thể chia sẻ dữ liệu được thu thập với các chi nhánh, nhà thầu phụ, nhà phân phối và các đối tác của mình nhưng luôn ở định dạng không thể xác định, ẩn danh.

Trở thành người đóng góp cho Mạng Bảo vệ Thời gian thực

Bạn có thể giúp chúng tôi nâng cao sự bảo vệ Mạng Bảo vệ Thời gian thực bằng cách đóng góp thông tin về các chương trình và trang web độc hại.

Bạn có thể chọn tham gia vào Mạng Bảo vệ Thời gian thực trong quá trình cài đặt. Với cài đặt mặc định của quá trình cài đặt, bạn đóng góp dữ liệu cho Mạng Bảo vệ Thời gian thực. Bạn có thể thay đổi cài đặt này sau trong sản phẩm.

Làm theo các chỉ dẫn sau đây để thay đổi cài đặt Mạng Bảo vệ Thời gian thực:

1. Trên bảng khởi chạy, nhấp phải vào biểu tượng ngoài cùng bên phải.
   Trình đơn bật lên xuất hiện.

2. Chọn **Mở cài đặt chung**.
3. Chọn **Cài đặt khác** > **Bảo mật**.
4. Chọn hộp kiểm tham gia để trở thành người đóng góp cho Mạng Bảo vệ Thời gian thực.

Câu hỏi về Mạng Bảo vệ Thời gian thực

Thông tin liên hệ về bất kỳ câu hỏi nào về Mạng Bảo vệ Thời gian thực.

Nếu bạn có bất kỳ câu hỏi nào khác về Mạng Bảo vệ Thời gian thực, vui lòng liên hệ:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

http://www.f-secure.com/en/web/home_global/support/contact

Phiên bản mới nhất của chính sách này luôn sẵn có trên trang web của chúng tôi.

Làm thế nào để biết đăng ký của tôi không hợp lệ

Loại và trạng thái đăng ký của bạn được hiển thị trên trang **Trạng thái đăng ký**.

Khi đăng ký sắp hết hạn hoặc nếu đăng ký của bạn đã hết hạn, trạng thái bảo vệ tổng thể của chương trìnhtrên biểu tượng bảng khởi chạy tương ứng thay đổi.

Để kiểm tra tính hợp lệ cho đăng ký của bạn:

1. Trên bảng khởi chạy, nhấp phải vào biểu tượng ngoài cùng bên phải.
   Trình đơn bật lên xuất hiện.
2. Chọn **Xem đăng ký của tôi**.
3. Chọn **Trạng thái đăng ký** để xem thông tin về đăng ký của bạn cho các chương trình đã cài đặt.
4. Chọn **Trạng thái cài đặt** để xem chương trình nào sẵn có để được cài đặt.

Trạng thái và ngày hết hạn của đăng ký của bạn cũng được hiển thị trên trang **Số liệu thống kê** của chương trình. Nếu đăng ký của bạn hết hạn, bạn cần phải gia hạn đăng ký của mình để tiếp tục nhận được các cập nhật và sử dụng sản phẩm.

Ghi chú: Khi đăng ký của bạn đã hết hạn, biểu tượng trạng thái sản phẩm nhấp nháy trên khay hệ thống của bạn.

Trung tâm hành động

Trung tâm hành động hiển thị cho bạn mọi thông báo quan trọng mà bạn cần chú ý.

Nếu đăng ký của bạn đã hết hạn hoặc sắp hết hạn, trung tâm hành động sẽ thông báo cho bạn về việc này. Màu nền và nội dung của thông báo trên trung tâm hành động phụ thuộc vào loại đăng ký và trạng thái của bạn:

- Nếu đăng ký của bạn sắp hết hạn và sẵn có đăng ký miễn phí, thông báo có nền màu trắng và nút **Kích hoạt**.

- Nếu đăng ký của bạn sắp hết hạn và không sẵn có đăng ký miễn phí, thông báo có nền màu vàng và các nút **Mua** và **Nhập mã**. Nếu bạn đã mua một đăng ký mới, bạn có thể nhấp vào **Nhập mã** để cung cấp mã đăng ký và kích hoạt đăng ký mới của mình.
- Nếu đăng ký của bạn đã hết hạn và sẵn có đăng ký miễn phí, thông báo có nền màu đỏ và nút **Kích hoạt**.
- Nếu đăng ký của bạn đã hết hạn và không sẵn có đăng ký miễn phí, thông báo có nền màu đỏ và các nút **Mua** và **Nhập mã**. Nếu bạn đã mua đăng ký mới, bạn có thể nhấp vào **Nhập mã** để cung cấp mã đăng ký và kích hoạt đăng ký mới của mình.

Ghi chú: Liên kết **Hiển thị lịch sử thông báo** trên trung tâm hành động hiển thị danh sách những thư thông báo sản phẩm, không phải những thư trên trung tâm hành động trước đây.

Kích hoạt đăng ký

Khi bạn có khoá đăng ký hoặc mã chiến dịch mới cho sản phẩm, bạn cần phải kích hoạt khoá đăng ký hoặc mã chiến dịch đó.

Để kích hoạt đăng ký:

1. Trên bảng khởi chạy, nhấp phải vào biểu tượng ngoài cùng bên phải.
   Trình đơn bật lên xuất hiện.
2. Chọn **Xem đăng ký của tôi**.
3. Chọn một trong hai tuỳ chọn sau:
   - Nhấp vào **Kích hoạt đăng ký**.
   - Nhấp vào **Kích hoạt mã chiến dịch**.
4. Trong hộp thoại mở, nhập khoá đăng ký mới hoặc mã chiến dịch của bạn và nhấp vào **OK**.

   Mẹo: Nếu bạn nhận được khoá đăng ký của mình qua e-mail, bạn có thể sao chép khoá này từ e-mail đó và dán vào trường này.

Sau khi bạn đã nhập khoá đăng ký mới, ngày hợp lệ của đăng ký mới được hiển thị trên trang **Trạng thái đăng ký**.

Chương

3

Giới thiệu

Chủ đề:

- *Xem toàn bộ trạng thái bảo vệ của tôi*
- *Xem thống kê sản phẩm*
- *Xử lý các bản cập nhật sản phẩm*
- *Vi-rút và phần mềm độc hại khác là gì*

Sản phẩm này bảo vệ máy tính của bạn khỏi vi-rút và các chương trình độc hại khác.

Sản phẩm tự động quét tệp, phân tích ứng dụng và cập nhật. Sản phẩm này không yêu cầu bất kỳ tác vụ nào từ bạn.

Xem toàn bộ trạng thái bảo vệ của tôi

Trang **Trạng thái** trình bày cho bạn một phần tổng quan nhanh về các tính năng sản phẩm đã cài đặt và trạng thái hiện tại của chúng.

Để mở trang **Trạng thái**:

Trên trang chính, nhấp **Trạng thái**.

Trang **Trạng thái** mở ra.

Các biểu tượng cho bạn biết trạng thái và các tính năng bảo mật của chương trình.

Biểu tượng trạng thái	Tên trạng thái	Mô tả
	OK	Máy tính của bạn được bảo vệ. Tính năng này được bật và hoạt động bình thường.
	Thông tin	Sản phẩm này thông báo cho bạn trạng thái đặc biệt của một tính năng. Ví dụ: tính năng đang được cập nhật.
	Cảnh báo	Máy tính của bạn không được bảo vệ đầy đủ. Ví dụ: sản phẩm không nhận được các bản cập nhật trong khoảng thời gian dài hoặc trạng thái của tính năng cần được chú ý.
	Lỗi	Máy tính của bạn không được bảo vệ. Ví dụ: đăng ký của bạn đã hết hạn hoặc tính năng quan trọng bị tắt.
	Tắt	Một tính năng không quan trọng bị tắt.

Xem thống kê sản phẩm

Bạn có thể xem các tác vụ sản phẩm đã thực hiện trên trang **Thống kê** kể từ khi sản phẩm được cài đặt.

Để mở trang **Thống kê**:

Trên trang chính, nhấp **Thống kê**.

Trang **Thống kê** mở ra.

- **Kiểm tra lần cập nhật thành công sau cùng** hiển thị thời gian cập nhật gần đây nhất.

- **Quét vi-rút và phần mềm gián điệp** hiển thị số tệp sản phẩm đã quét và xoá kể từ khi cài đặt.
- **Ứng dụng** hiển thị số chương trình DeepGuard cho phép hoặc chặn kể từ khi cài đặt.
- **Kết nối tường lửa** hiển thị số kết nối được phép và bị chặn kể từ khi cài đặt.
- **Lọc thư rác và thư lừa đảo** hiển thị số lượng thư e-mail mà sản phẩm đã phát hiện dưới dạng thư e-mail hợp lệ và dưới dạng thư rác.

Xử lý các bản cập nhật sản phẩm

Sản phẩm tự động được cập nhật bảo vệ.

Xem phiên bản cơ sở dữ liệu

Bạn có thể xem những lần cập nhật và số phiên bản mới nhất trong trang **Cập nhật cơ sở dữ liệu**.

Để mở trang **Cập nhật cơ sở dữ liệu**:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Cài đặt khác** > **Phiên bản cơ sở dữ liệu**.

Trang **Phiên bản cơ sở dữ liệu** hiển thị ngày mới nhất khi các định nghĩa vi-rút và phần mềm gián điệp, DeepGuard và bộ lọc thư rác và thư lừa đảo được cập nhật và số phiên bản của chúng.

Thay đổi cài đặt băng thông rộng di động

Chọn xem bạn có muốn tải xuống các cập nhật bảo mật khi bạn sử dụng băng thông rộng di động hay không.

Ghi chú: Tính năng này chỉ có sẵn trong Microsoft Windows 7.

Theo mặc định, các cập nhật bảo mật luôn được tải xuống khi bạn trong mạng của nhà cung cấp mạng mạng chủ. Tuy nhiên, các cập nhật bị tạm dừng khi bạn truy cập vào mạng của nhà cung cấp khác. Lý do là chi phí kết nối có thể khác nhau giữa các nhà cung cấp, chẳng hạn như ở những quốc gia khác nhau. Bạn có thể xem xét việc giữ nguyên cài đặt này, nếu bạn muốn tiết kiệm băng thông và cũng có thể chi phí, trong khi bạn truy cập.

Ghi chú: Cài đặt này chỉ áp dụng cho kết nối băng thông rộng di động. Khi máy tính được kết nối với mạng cố định hoặc không dây, sản phẩm được cập nhật tự động.

Để thay đổi cài đặt:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Cài đặt khác** > **Băng thông rộng di động** > **Tải xuống bản cập nhật bảo mật**.
3. Chọn tuỳ chọn cập nhật ưa thích cho kết nối di động:
   - **Chỉ trong mạng của nhà cung cấp chính của tôi**

     Các cập nhật luôn được tải xuống trong mạng nhà cung cấp mạng chủ của bạn. Khi bạn truy cập vào mạng của nhà cung cấp khác, các cập nhật sẽ bị tạm dừng. Chúng tôi khuyên bạn nên chọn tuỳ chọn này để luôn cập nhật sản phẩm bảo mật của mình ở mức chi phí mong muốn.
   - **Không bao giờ**

     Bản cập nhật không được tải xuống khi bạn sử dụng băng thông rộng di động.
   - **Luôn luôn**

Các cập nhật luôn được tải xuống, bất kể bạn đang sử dụng mạng gì. Chọn tuỳ chọn này nếu bạn muốn đảm bảo rằng bảo mật máy tính của bạn luôn được cập nhật mà không tính đến chi phí.

4. Nếu bạn muốn quyết định riêng mỗi khi bạn thoát khỏi mạng của nhà cung cấp mạng chủ của mình, chọn **Hỏi mỗi khi bạn thoát khỏi mạng của nhà cung cấp mạng chủ của bạn**.

Bản cập nhật bảo mật bị tạm dừng

Bản cập nhật bảo mật có thể bị tạm dừng khi bạn sử dụng băng thông rộng di động bên ngoài mạng của nhà cung cấp dịch vụ mạng chủ của bạn.

Trong trường hợp này, bạn có thể thấy bảng thông báo **Bị tạm dừng** ở góc dưới bên phải của màn hình của mình. Bản cập nhật bị tạm dừng vì chi phí kết nối có thể khác nhau giữa các nhà cung cấp, chẳng hạn như ở các quốc gia khác nhau. Bạn có thể xem xét việc giữ nguyên cài đặt này, nếu bạn muốn tiết kiệm băng thông và cũng có thể là chi phí, trong khi bạn truy cập. Tuy nhiên, nếu bạn vẫn muốn thay đổi cài đặt, hãy nhấp vào liên kết **Thay đổi**.

Ghi chú:

Tính năng này chỉ có sẵn trong Microsoft Windows 7.

Vi-rút và phần mềm độc hại khác là gì

Phần mềm độc hại là các chương trình được thiết kế cụ thể nhằm gây thiệt hại cho máy tính của bạn, sử dụng máy tính của bạn cho mục đích bất hợp pháp mà bạn không biết hoặc đánh cắp thông tin từ máy tính của bạn.

Phần mềm độc hại có thể:

- kiểm soát trình duyệt web của bạn,
- chuyển hướng nỗ lực tìm kiếm của bạn,
- hiển thị quảng cáo không mong muốn,
- theo dõi các trang web bạn truy cập,
- đánh cắp thông tin cá nhân chẳng hạn như thông tin ngân hàng,
- sử dụng máy tính của bạn để gửi spam và
- sử dụng máy tính của bạn để tấn công những máy tính khác.

Phần mềm độc hại cũng có thể khiến máy tính của bạn trở nên chậm và không ổn định. Bạn có thể nghi ngờ máy tính của bạn có*phần mềm độc hại* nếu đột nhiên máy tính trở nên rất chậm hoặc thường xuyên bị lỗi.

Vi-rút

Vi-rút thường là các chương trình có thể tự tấn công các tệp và liên tục tự tái tạo; chúng có thể thay đổi và thay thế nội dung của các tệp khác theo cách có thể gây hại cho máy tính của bạn.

Vi-rút là chương trình thường được cài đặt vào máy tính của bạn mà bạn không biết. Khi đã có trong máy tính, vi-rút sẽ tìm cách tự tái tạo. Vi-rút:

- sử dụng một số tài nguyên hệ thống của máy tính của bạn,
- có thể thay đổi hoặc làm hỏng các tệp trên máy tính của bạn,
- có thể cố sử dụng máy tính của bạn để lây lan sang các máy tính khác,
- có thể sử dụng máy tính của bạn cho mục đích bất hợp pháp.

Phần mềm gián điệp

Phần mềm gián điệp là các chương trình thu thập thông tin cá nhân của bạn.

Phần mềm gián điệp có thể thu thập thông tin cá nhân bao gồm:

- các trang web trên Internet mà bạn đã duyệt qua,
- địa chỉ e-mail từ máy tính của bạn,
- mật khẩu hoặc
- số thẻ tín dụng.

Phần mềm gián điệp gần như luôn tự cài đặt mà không cần sự cho phép rõ ràng của bạn. Phần mềm gián điệp có thể được cài đặt cùng với một chương trình hữu ích hoặc bằng cách lừa bạn nhấp vào một tuỳ chọn trong cửa sổ bật lên giả mạo.

Rootkit

Rootkit là các chương trình khiến việc tìm kiếm *phần mềm độc hại* khác trở nên khó khăn.

Rootkit ẩn các tệp và quá trình. Nhìn chung, chúng thực hiện việc này để ẩn hoạt động có hại trên máy tính của bạn. Khi rootkit ẩn *phần mềm độc hại*, bạn khó có thể phát hiện ra rằng máy tính của bạn có phần mềm độc hại.

Sản phẩm này có trình quét rootkit, đặc biệt quét rootkit, vì vậy *phần mềm độc hại* không thể dễ dàng tự ẩn.

Phần mềm nguy hiểm

Phần mềm nguy hiểm không được thiết kế cụ thể để làm hại máy tính của bạn, nhưng nó có thể gây hại cho máy tính của bạn nếu bạn sử dụng sai.

Phần mềm nguy hiểm không hẳn là phần mềm độc hại. Các chương trình của phần mềm nguy hiểm thực hiện một số chức năng hữu ích nhưng tiềm ẩn nguy hiểm.

Ví dụ về các chương trình phần mềm nguy hiểm là:

- các chương trình để nhắn tin nhanh, như IRC (Trò chuyện Luân phiên trên Internet),
- các chương trình để chuyển tệp qua Internet từ máy tính này sang máy tính khác,
- Các chương trình gọi điện thoại qua Internet, như VoIP (*Đàm thoại qua Giao thức Internet*),
- Phần mềm Truy cập Từ xa, như VNC,
- phần mềm gián điệp, có thể tìm cách đe doạ hoặc dụ dỗ mọi người mua phần mềm bảo mật giả mạo hoặc
- phần mềm được thiết kế để bỏ qua kiểm tra CD hoặc bảo vệ sao chép.

Nếu bạn đã cài đặt chương trình và thiết lập đúng, chương trình ít có khả năng gây hại hơn.

Nếu phần mềm nguy hiểm được cài đặt mà bạn không biết, có nhiều khả năng chương trình được cài đặt với mục đích xấu và cần xoá bỏ.

Chương

4

Bảo vệ máy tính của bạn khỏi phần mềm độc hại

Chủ đề:

- *Cách quét máy tính của tôi*
- *Cách loại trừ tệp khỏi quá trình quét*
- *Cách sử dụng khu vực cách ly*
- *DeepGuard là gì*

Quét vi-rút và phần mềm gián điệp sẽ bảo vệ máy tính của bạn khỏi các chương trình có thể đánh cắp thông tin cá nhân của bạn, làm hỏng máy chủ hoặc sử dụng cho mục đích bất hợp pháp.

Theo mặc định, tất cả các loại phần mềm độc hại ngay lập tức bị xử lý khi chúng được phát hiện, để chúng không thể gây hại.

Theo mặc định, quét vi-rút và phần mềm gián điệp sẽ tự động quét ổ đĩa cứng cục bộ, mọi phương tiện di động (như đĩa di động hoặc đĩa nén) và nội dung được tải xuống. Đồng thời, bạn cũng có thể đặt tự động quét e-mail.

Quét vi-rút và phần mềm gián điệp cũng giám sát mọi thay đổi cho máy tính của bạn có thể cho biết *phần mềm độc hại*. Nếu phát hiện thấy bất kỳ thay đổi nào gây nguy hiểm cho hệ thống, chẳng hạn như cài đặt hệ thống hoặc nỗ lực thay đổi các quá trình quan trọng của hệ thống, DeepGuard sẽ ngăn không cho chương trình này chạy vì đó có thể là *phần mềm độc hại*.

Cách quét máy tính của tôi

Khi Quét vi-rút và phần mềm gián điệp được bật, Quét vi-rút và phần mềm gián điệp tự động quét các tệp độc hại trên máy tính của bạn. Bạn cũng có thể quét các tệp một cách thủ công và thiết lập quá trình quét theo lịch.

Chúng tôi khuyên bạn luôn luôn nên bật Quét vi-rút và phần mềm gián điệp. Quét tệp một cách thủ công khi bạn muốn đảm bảo rằng không có tệp độc hại nào trên máy tính của mình hoặc nếu bạn muốn quét tệp mà bạn đã loại trừ khỏi quá trình quét trong thời gian thực.

Bằng cách thiết lập quá trình quét được lập lịch biểu, Quét vi-rút và phần mềm gián điệp xoá các tệp độc hại khỏi máy tính của bạn tại những thời điểm được chỉ định.

Quét tệp một cách tự động

Quét trong thời gian thực bảo vệ máy tính của bạn bằng cách quét tất cả các tệp khi chúng được truy cập và bằng cách chặn truy cập vào những tệp chứa *phần mềm độc hại*.

Khi máy tính của bạn cố truy cập vào một tệp, Quét trong thời gian thực quét phần mềm độc hại cho tệp trước khi cho phép máy tính của bạn truy cập vào tệp đó. Nếu Quét trong thời gian thực tìm thấy bất kỳ nội dung độc hại nào, Quét trong thời gian thực sẽ cách ly tệp trước khi tệp có thể gây ra gây hại.

Quét trong thời gian thực có ảnh hưởng đến hiệu suất của máy tính của tôi không?

Thông thường, bạn không biết quá trình quét vì nó chỉ mất một ít thời gian và tài nguyên hệ thống. Ví dụ: lượng thời gian và tài nguyên hệ thống mà quá trình quét trong thời gian thực cần tuỳ thuộc vào nội dung, vị trí và loại tệp.

Các tệp mất nhiều thời gian hơn để quét:

- Tệp trên ổ đĩa CD, DVD và ổ đĩa USB di động.
- Tệp nén, như *các tệp*.zip.

  Ghi chú: Tệp bị nén không được quét theo mặc định.

Quét trong thời gian thực có thể làm chậm máy tính của bạn nếu:

- bạn có máy tính không đáp ứng các yêu cầu hệ thống hoặc
- bạn truy cập vào nhiều tệp cùng một lúc. Ví dụ: khi bạn mở thư mục chứa nhiều tệp cần được quét.

Bật hoặc tắt chương trình quét trong thời gian thực

Bật tính năng quét trong thời gian thực để dừng *phần mềm độc hại* trước khi phần mềm độc hại đó có thể gây hại cho máy tính của bạn.

Để bật hoặc tắt tính năng quét trong thời gian thực:

1. Trên trang chính, nhấp **Trạng thái**.
2. Nhấp vào **Thay đổi cài đặt trên trang này**.

   Ghi chú: Bạn cần quyền quản trị để tắt các tính năng bảo mật.

3. Bật hoặc tắt **Quét vi-rút và phần mềm gián điệp**.
4. Nhấp vào **Đóng**.

Tự động xử lý các tệp có hại

Tính năng quét trong thời gian thực có thể tự động xử lý các tệp có hại mà không hỏi bạn bất kỳ câu hỏi nào.

Để cho phép tính năng quét trong thời gian thực tự động xử lý các tệp có hại:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Bảo mật Máy tính** > **Quét vi-rút và phần mềm gián điệp**.
3. Chọn **Tự động xử lý các tệp có hại**.

Nếu bạn chọn không tự động xử lý các tệp có hại, tính năng quét trong thời gian thực hỏi bạn việc cần thực hiện đối với tệp có hại khi được tìm thấy.

Xử lý phần mềm gián điệp

Quét vi-rút và phần mềm gián điệp chặn phần mềm gián điệp ngay lập tức khi phần mềm gián điệp cố khởi động.

Trước khi ứng dụng phần mềm gián điệp có thể khởi động, sản phẩm chặn ứng dụng đó và cho phép bạn quyết định những việc bạn muốn thực hiện với ứng dụng đó.

Chọn một trong các tác vụ sau đây khi tìm thấy phần mềm gián điệp:

Tác vụ cần thực hiện	Điều gì xảy ra với phần mềm gián điệp
Tự động xử lý	Cho phép sản phẩm quyết định tác vụ tốt nhất cần thực hiện dựa trên phần mềm gián điệp được tìm thấy.
Cách ly phần mềm gián điệp	Chuyển phần mềm gián điệp đến mục cách ly nơi phần mềm gián điệp này không thể gây hại cho máy tính của bạn.
Xoá phần mềm gián điệp	Xoá tất cả các tệp có liên quan đến phần mềm gián điệp khỏi máy tính của bạn.
Chỉ chặn phần mềm gián điệp	Chặn quyền truy cập vào phần mềm gián điệp nhưng để phần mềm đó lên máy tính của bạn.
Loại trừ phần mềm gián điệp khỏi quá trình quét	Cho phép phần mềm gián điệp chạy và loại trừ phần mềm gián điệp đó khỏi quá trình quét trong tương lai.

Xử lý phần mềm nguy hiểm

Quét vi-rút và phần mềm gián điệp chặn phần mềm nguy hiểm ngay lập tức khi phần mềm nguy hiểm đó cố khởi động.

Trước khi ứng dụng phần mềm nguy hiểm có thể khởi động, sản phẩm chặn ứng dụng đó và cho phép bạn quyết định những việc bạn muốn thực hiện với ứng dụng đó.

Chọn một trong các tác vụ sau đây khi tìm thấy phần mềm nguy hiểm:

Tác vụ cần thực hiện	Điều gì xảy ra với phần mềm nguy hiểm
Chỉ chặn phần mềm nguy hiểm	Chặn quyền truy cập vào phần mềm nguy hiểm nhưng để phần mềm đó lên máy tính của bạn.
Cách ly phần mềm nguy hiểm	Chuyển phần mềm nguy hiểm đến mục cách ly nơi phần mềm nguy hiểm không thể gây hại cho máy tính của bạn.
Xoá phần mềm nguy hiểm	Xoá tất cả các tệp có liên quan đến phần mềm nguy hiểm khỏi máy tính của bạn.
Loại trừ phần mềm nguy hiểm khỏi quá trình quét	Cho phép phần mềm nguy hiểm chạy và loại trừ phần mềm nguy hiểm đó khỏi quá trình quét trong tương lai.

Tự động xoá các cookie theo dõi

Bằng cách xoá cookie theo dõi, bạn sẽ chặn các trang web có thể theo dõi trang web mà bạn truy cập trên Internet.

Cookie theo dõi là những tệp nhỏ cho phép trang web ghi lại những trang web mà bạn truy cập. Làm theo các hướng dẫn để xoá các cookie theo dõi khỏi máy tính của bạn.

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Bảo mật Máy tính** > **Quét vi-rút và phần mềm gián điệp**.
3. Chọn **Xoá cookie theo dõi**.
4. Nhấp vào **OK**.

Quét tệp một cách thủ công

Khi bạn quét tệp của mình một cách thủ công, ví dụ: khi bạn kết nối thiết bị bên ngoài với máy tính của mình, để đảm bảo rằng tệp không chứa bất kỳ phần mềm độc hại nào.

Bắt đầu quá trình quét thủ công

Bạn có thể quét toàn bộ máy tính hoặc quét một loại *phần mềm độc hại* cụ thể hoặc một vị trí cụ thể.

Nếu bạn nghi ngờ về một loại *phần mềm độc hại* nhất định, bạn có thể chỉ quét loại đó. Nếu bạn nghi ngờ về một vị trí nhất định trên máy tính, bạn có thể chỉ quét vị trí đó. Quá trình quét này sẽ kết thúc nhanh hơn việc quét toàn bộ máy tính của bạn.

Để bắt đầu quét máy tính theo cách thủ công:

1. Trên trang chính, nhấp vào mũi tên bên dưới **Quét**.

   Các tuỳ chọn quét được hiển thị.

2. Chọn loại chế độ quét.

   Chọn **Thay đổi cài đặt quét** để tối ưu hoá cách quá trình quét thủ công quét vi-rút và các ứng dụng có hại khác trên máy tính của bạn.

3. Nếu bạn chọn **Chọn vị trí để quét**, một cửa sổ mở ra, trong đó bạn có thể chọn vị trí để quét. **Thuật sỹ Quét** mở ra.

Các loại chế độ quét

Bạn có thể quét toàn bộ máy tính hoặc quét loại phần mềm độc hại cụ thể hoặc một vị trí cụ thể.

Phần sau liệt kê các loại chế độ quét khác nhau:

Loại chế độ quét	Nội dung được quét	Khi nào thì sử dụng loại này
Quét vi-rút và phần mềm gián điệp	Các phần của máy tính của bạn để tìm vi-rút, phần mềm gián điệp và phần mềm nguy hiểm	Loại chế độ quét này nhanh hơn nhiều so với quét toàn bộ. Loại chế độ quét này chỉ tìm kiếm các phần của hệ thống có chứa các tệp chương trình được cài đặt. Loại chế độ quét này được khuyên dùng nếu bạn muốn kiểm tra một cách nhanh chóng xem máy tính của bạn có sạch không, vì nó có thể tìm và xoá một cách hiệu quả phần mềm độc hại đang hoạt động trên máy tính của bạn.
Quét toàn bộ máy tính	Toàn bộ máy tính của bạn (ổ đĩa cứng bên trong và bên ngoài) đối	Khi bạn muốn hoàn toàn chắc chắn rằng không có phần mềm độc hại hoặc phần mềm nguy hiểm trên máy tính của bạn. Loại chế độ quét này mất nhiều thời gian nhất

Loại chế độ quét	Nội dung được quét	Khi nào thì sử dụng loại này
	với vi-rút, phần mềm gián điệp và phần mềm nguy hiểm	để hoàn thành. Loại chế độ quét này bao gồm quét nhanh phần mềm độc hại và quét ổ đĩa cứng. Nó cũng kiểm tra các mục có thể bị ẩn bởi rootkit.
Chọn những gì cần quét	Tệp, thư mục hoặc ổ đĩa cụ thể để tìm vi-rút, phần mềm gián điệp và phần mềm nguy hiểm	Khi bạn nghi ngờ một vị trí cụ thể trên máy tính của mình có thể có phần mềm độc hại, ví dụ: vị trí chứa các mục tải xuống từ những nguồn có thể nguy hiểm, như mạng chia sẻ tệp ngang hàng. Thời gian quét sẽ tuỳ thuộc vào kích thước của đích bạn muốn quét. Ví dụ: quét sẽ nhanh chóng hoàn tất nếu bạn quét một thư mục chỉ chứa một vài tệp nhỏ.
Quét rootkit	Các vị trí hệ thống quan trọng, tại đó mục nghi ngờ có thể là vấn đề bảo mật. Quét các tệp, thư mục bị ẩn, ổ đĩa hoặc quá trình	Khi bạn nghi ngờ rằng rootkit có thể được cài đặt trên máy tính của mình. Ví dụ: nếu phần mềm độc hại vừa được phát hiện trong máy tính của bạn và bạn muốn đảm bảo rằng nó không cài đặt một rootkit.

Quét trong Windows Explorer

Bạn cũng có thể quét *vi-rút*, *phần mềm gián điệp* và *phần mềm nguy hiểm* cho các đĩa, thư mục và tệp trong Windows Explorer.

Để quét đĩa, thư mục hoặc tệp:

1. Đặt con trỏ chuột lên và nhấp chuột phải vào đĩa, thư mục hoặc tệp bạn muốn quét.
2. Từ menu chuột phải, chọn **Quét Vi-rút cho Thư mục** (tên tuỳ chọn phụ thuộc vào việc liệu bạn có đang quét đĩa, thư mục hay tệp không).
   Cửa sổ **Thuật sĩ Quét** mở ra và quá trình quét bắt đầu.

Nếu phát hiện *vi-rút* hoặc *phần mềm gián điệp* thì **Thuật sĩ Quét** sẽ hướng dẫn bạn qua các giai đoạn xoá.

Chọn tệp cần quét

Bạn có thể chọn các loại tệp mà bạn muốn quét *vi-rút* và *phần mềm gián điệp* trong các quá trình quét thủ công và theo lịch.

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Cài đặt khác** > **Quét thủ công**.
3. Trong **Tuỳ chọn quét**, hãy chọn trong số các cài đặt sau đây:

Chỉ quét các loại tệp xác định	Để chỉ quét những loại tệp có nhiều khả năng bị nhiễm nhất, chẳng hạn như các tệp thi hành. Việc chọn tuỳ chọn này cũng khiến quá trình quét diễn ra nhanh hơn. Các tệp có đuôi mở rộng sau được quét: `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` và `.hqx`.
Quét trong các tệp nén	Để quét các tệp và thư mục lưu trữ

Sử dụng suy nghiệm nâng cao	Để sử dụng tất cả các quét phỏng đoán có sẵn trong khi quét để tìm hiệu quả hơn phần mềm độc hại mới hoặc chưa biết. **Ghi chú:** Nếu bạn chọn tuỳ chọn này, quá trình quét diễn ra lâu hơn và có thể dẫn đến nhiều cảnh báo nhầm hơn (các tệp vô hại được báo cáo là đáng ngờ).

4. Nhấp vào **OK**.

Ghi chú: Các tệp được loại trừ trên danh sách mục được loại trừ không được quét ngay cả khi bạn chọn quét chúng tại đây.

Tác vụ cần thực hiện khi tìm thấy các tệp độc hại

Chọn cách bạn muốn xử lý các tệp độc hại khi tìm thấy chúng.

Để chọn tác vụ cần thực hiện khi tìm thấy nội dung độc hại trong quá trình quét thủ công:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Cài đặt khác** > **Quét thủ công**.
3. Trong **Khi phát hiện vi-rút hoặc phần mềm gián điệp**, hãy chọn một trong các tuỳ chọn sau đây:

Tuỳ chọn	Mô tả
Hỏi tôi (mặc định)	Bạn có thể chọn tác vụ cần thực hiện cho mọi mục được tìm thấy trong quá trình quét thủ công.
Làm sạch tệp	Sản phẩm cố tự động diệt các tệp bị nhiễm được tìm thấy trong quá trình quét thủ công. **Ghi chú:** Nếu sản phẩm không thể làm sạch tệp bị nhiệm, tệp sẽ bị cách ly (ngoại trừ được tìm thấy trên mạng hoặc trên các ổ di động) do đó tệp không gây hại cho máy tính.
Cách ly tệp	Sản phẩm chuyển bất kỳ mục có hại nào được tìm thấy trong quá trình quét thủ công vào mục cách ly nơi chúng không thể gây hại cho máy tính.
Xoá tệp	Sản phẩm xoá bất kỳ tệp có hại nào được tìm thấy trong quá trình quét thủ công.
Chỉ báo cáo	Sản phẩm để lại bất kỳ tệp có hại nào được tìm thấy trong quá trình quét thủ công như vốn có và ghi lại việc phát hiện trong báo cáo quét. **Ghi chú:** Nếu chức năng quét theo thời gian thực bị tắt, bất kỳ phần mềm gián điệp nào cũng có thể gây hại cho máy tính nếu bạn chọn tuỳ chọn này.

Ghi chú: Khi các tệp có hại được tìm thấy trong quá trình quét theo lịch, chúng được tự động làm sạch.

Đặt lịch quét

Đặt máy tính của bạn tự động quét và xoá vi-rút và các ứng dụng độc hại khác khi bạn sử dụng máy tính hoặc đặt quá trình quét chạy định kỳ để đảm bảo máy tính của bạn sạch.

Để đặt lịch quét:

1. Trên trang chính, nhấp **Cài đặt**.

Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Cài đặt khác** > **Quét theo lịch**.
3. Bật **Quét theo lịch**.
4. Chọn thời điểm bạn muốn quá trình quét bắt đầu.

Tuỳ chọn	Mô tả
Hàng ngày	Quét máy tính của bạn hàng ngày.
Hàng tuần	Quét máy tính của bạn vào những ngày được chọn trong tuần. Chọn ngày từ danh sách.
Hàng tháng	Quét máy tính của bạn vào những ngày được chọn trong tháng. Để chọn ngày: 1. Chọn một trong số các tuỳ chọn **Ngày**. 2. Chọn ngày trong tháng từ danh sách bên cạnh ngày đã chọn.

5. Chọn thời điểm bạn muốn bắt đầu quét vào ngày đã chọn.

Tuỳ chọn	Mô tả
Thời gian bắt đầu	Bắt đầu quá trình quét tại thời điểm được chỉ định.
Sau khi máy tính không được sử dụng trong	Bắt đầu quá trình quét sau khi bạn không sử dụng máy tính của mình trong khoảng thời gian được chỉ định.

Quét theo lịch sử dụng cài đặt quét thủ công khi quét máy tính của bạn, ngoại trừ khi quét các lưu trữ mỗi lần và tự động làm sạch các tệp độc hại.

Quét e-mail

Tính năng quét e-mail bảo vệ bạn khỏi các tệp có hại trong e-mail được gửi đến bạn.

Tính năng quét vi-rút và phần mềm gián điệp phải được bật để quét vi-rút cho e-mail.

Để bật quét e-mail:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Bảo mật Máy tính** > **Quét vi-rút và phần mềm gián điệp**.
3. Chọn **Xoá tệp đính kèm e-mail có hại**.
4. Nhấp vào **OK**.

Khi nào thư e-mail và tệp đính kèm được quét

Quét vi-rút và phần mềm gián điệp có thể xoá bỏ nội dung độc hại khỏi e-mail bạn nhận được.

Tính năng quét vi-rút và phần mềm gián điệp xoá thư e-mail độc hại được nhận bằng các chương trình e-mail, chẳng hạn như Microsoft Outlook và Outlook Express, Microsoft Mail hoặc Mozilla Thunderbird. Tính năng này quét thư e-mail và tệp đính kèm không được mã hoá mỗi khi chương trình e-mail của bạn nhận được chúng từ máy chủ thư bằng cách sử dụng giao thức POP3.

Quét vi-rút và phần mềm gián điệp không thể quét thư e-mail trong thư trên web, bao gồm các ứng dụng e-mail chạy trong trình duyệt web của bạn, chẳng hạn như Hotmail, Yahoo! mail hoặc Gmail. Bạn vẫn được bảo vệ khỏi *vi-rút* ngay cả khi bạn không xoá tệp đính kèm có hại hoặc khi bạn đang sử dụng thư trên web. Khi bạn mở tệp đính kèm e-mail, quét trong thời gian thực sẽ xoá bất kỳ tệp đính kèm gây hại nào trước khi chúng có thể gây hại.

Ghi chú: Quét trong thời gian thực chỉ bảo vệ máy tính của bạn, chứ không bảo vệ bạn bè của bạn. Quét trong thời gian thực không quét tệp được đính kèm trừ khi bạn mở tệp đính kèm. Điều này có nghĩa là nếu bạn đang sử dụng thư trên web và bạn chuyển tiếp thư trước khi mở tệp đính kèm của thư đó, bạn có thể chuyển tiếp e-mail bị nhiễm vi-rút cho bạn bè của mình.

Xem kết quả quét

Lịch sử vi-rút và phần mềm gián điệp hiển thị tất cả các tệp có hại mà sản phẩm đã tìm thấy.

Đôi khi sản phẩm không thể thực hiện tác vụ bạn đã chọn khi nội dung có hại nào đó được phát hiện. Ví dụ: nếu bạn chọn làm sách tệp và tệp không thể được làm sạch, sản phẩm chuyển tệp đó đến mục cách ly. Bạn có thể xem thông tin này trong lịch sử vi-rút và phần mềm gián điệp.

Để xem lịch sử:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Bảo mật Máy tính** > **Quét vi-rút và phần mềm gián điệp**.
3. Nhấp vào **Xem lịch sử xoá**.

Lịch sử vi-rút và phần mềm gián điệp hiển thị thông tin sau đây:

- ngày và giờ tìm thấy tệp có hại,
- tên của phần mềm độc hại và vị trí của phần mềm độc hại đó trên máy tính của bạn và
- tác vụ đã thực hiện.

Cách loại trừ tệp khỏi quá trình quét

Đôi khi bạn có thể muốn loại trừ một số tệp hoặc ứng dụng khỏi quá trình quét. Các mục được loại trừ sẽ không được quét trừ khi bạn xoá chúng khỏi danh sách mục được loại trừ.

Ghi chú: Danh sách loại trừ tách biệt khỏi quá trình quét trong thời gian thực và thủ công. Ví dụ: nếu bạn loại trừ khỏi quá trình quét trong thời gian thực, tệp được quét trong quá trình quét thủ công trừ khi bạn cũng loại trừ tệp đó khỏi quá trình quét thủ công.

Loại trừ các loại tệp

Khi bạn loại trừ tệp theo loại của tệp, các tệp có tiện ích mở rộng được chỉ định không được quét nội dung có hại.

Để thêm hoặc xoá loại tệp bạn muốn loại trừ:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn xem bạn muốn loại trừ loại tệp đó khỏi quá trình quét trong thời gian thực hay quá trình quét thủ công:
   - Chọn **Bảo mật Máy tính** > **Quét vi-rút và phần mềm gián điệp** để loại trừ loại tệp khỏi quá trình quét trong thời gian thực.
   - Chọn **Cài đặt khác** > **Quét thủ công** để loại trừ loại tệp khỏi quá trình quét thủ công.
3. Nhấp vào **Loại trừ tệp khỏi quá trình quét**.
4. Để loại trừ một loại tệp:

a) Chọn tab **Loại Tệp**.
b) Chọn **Loại trừ tệp có đuôi mở rộng này**.
c) Nhập đuôi mở rộng tệp xác định loại tệp mà bạn muốn loại trừ, trong trường bên cạnh nút **Thêm**.

   Để sử dụng tệp không có đuôi mở rộng, nhập '.'. Bạn có thể sử dụng ký tự đại diện '?' để biểu thị bất kỳ ký tự đơn nào hoặc '*' để biểu thị bất kỳ số lượng ký tự nào.

   Ví dụ: để loại trừ các tệp thi hành, nhập exe vào trường.
d) Nhấp vào **Thêm**.

5. Lặp lại các bước trước đó đối với bất kỳ đuôi mở rộng nào khác bạn muốn được loại trừ khỏi quá trình quét vi-rút.
6. Nhấp vào **OK** để đóng hộp thoại **Loại trừ khỏi quá trình quét**.
7. Nhấp vào **OK** để áp dụng cài đặt mới.

Các loại tệp được chọn được loại trừ khỏi quá trình quét trong tương lai.

Loại trừ tệp theo vị trí

Khi bạn loại trừ tệp theo vị trí, các tệp trong các ổ hoặc thư mục được chỉ định không được quét nội dung có hại.

Để thêm hoặc xoá các vị trí tệp mà bạn muốn loại trừ:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn xem bạn muốn loại trừ vị trí khỏi quá trình quét trong thời gian thực hay quá trình quét thủ công:
   - Chọn **Máy tính** > **Quét vi-rút và phần mềm gián điệp** để loại trừ vị trí khỏi quá trình quét trong thời gian thực.
   - Chọn **Máy tính** > **Quét thủ công** để loại trừ vị trí khỏi quá trình quét thủ công.
3. Nhấp vào **Loại trừ tệp khỏi quá trình quét**.
4. Để loại trừ một tệp, ổ đĩa hoặc thư mục:
   a) Chọn tab **Đối tượng**.
   b) Chọn **Loại trừ các đối tượng (tệp, thư mục, ...)**.
   c) Nhấp **Thêm**.
   d) Chọn tệp, ổ đĩa hoặc thư mục mà bạn muốn loại trừ khỏi quá trình quét vi-rút.

      Ghi chú: Một số ổ đĩa có thể là các ổ đĩa di động, như CD, DVD hoặc ổ đĩa mạng. Không thể loại trừ ổ đĩa mạng hoặc ổ đĩa di động trống.

   e) Nhấp vào **OK**.
5. Lặp lại bước trước đó để loại trừ các tệp, ổ đĩa hoặc thư mục khác khỏi quá trình quét vi-rút.
6. Nhấp vào **OK** để đóng hộp thoại **Loại trừ khỏi quá trình quét**.
7. Nhấp vào **OK** để áp dụng cài đặt mới.

Các tệp, ổ hoặc thư mục được chọn được loại trừ khỏi quá trình quét trong tương lai.

Xem các ứng dụng được loại trừ

Bạn có thể xem các ứng dụng mà bạn đã loại trừ khỏi quá trình quét và xoá chúng khỏi danh sách mục được loại trừ nếu bạn muốn quét chúng trong tương lai.

Nếu tính năng quét trong thời gian thực hoặc thủ công phát hiện thấy ứng dụng thực hiện giống như phần mềm gián điệp hoặc phần mềm nguy hiểm nhưng bạn biết ứng dụng đó là an toàn, bạn có thể loại trừ ứng dụng đó khỏi quá trình quét để sản phẩm không cảnh báo cho bạn về ứng dụng đó nữa.

Ghi chú: Không thể loại trừ ứng dụng nếu ứng dụng đó thực hiện giống như vi-rút hoặc phần mềm độc hại khác.

Bạn không thể trực tiếp loại trừ các ứng dụng. Các ứng dụng mới chỉ xuất hiện trên danh sách loại trừ nếu bạn loại trừ chúng khỏi quá trình quét.

Để xem các ứng dụng được loại trừ khỏi quá trình quét:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn xem bạn muốn xem các ứng dụng đã được loại trừ khỏi quá trình quét trong thời gian thực hay quá trình quét thủ công:
   - Chọn **Máy tính** > **Quét vi-rút và phần mềm gián điệp** để xem các ứng dụng đã được loại trừ khỏi quá trình quét trong thời gian thực.
   - Chọn **Máy tính** > **Quét thủ công** để xem các ứng dụng đã được loại trừ khỏi quá trình quét thủ công.
3. Nhấp vào **Loại trừ tệp khỏi quá trình quét**.
4. Chọn tab **Ứng dụng**.

   Ghi chú: Chỉ có thể loại trừ các ứng dụng phần mềm gián điệp và phần mềm nguy hiểm, chứ không thể loại trừ vi-rút.

5. Nếu bạn muốn quét lại ứng dụng được loại trừ:
   a) Chọn ứng dụng bạn muốn đưa vào quá trình quét.
   b) Nhấp vào **Xoá**.
6. Nhấp vào **OK** để đóng hộp thoại **Loại trừ khỏi quá trình quét**.
7. Nhấp vào **OK** để thoát.

Cách sử dụng khu vực cách ly

Khu vực cách ly là hệ thống lưu trữ an toàn cho các tệp có thể gây hại.

Các tệp bị cách ly không thể lan truyền hoặc gây hại cho máy tính của bạn.

Sản phẩm có thể cách ly *phần mềm độc hại*, *phần mềm gián điệp* và *phần mềm nguy hiểm* để biến chúng thành vô hại. Bạn có thể khôi phục các ứng dụng hoặc tệp từ khu vực cách ly nếu bạn cần chúng.

Nếu bạn không cần mục đã cách ly, bạn có thể xoá mục đó. Việc xoá một mục trong khu vực cách ly sẽ xoá vĩnh viễn mục đó khỏi máy tính của bạn.

- Nhìn chung, bạn có thể xoá *phần mềm độc hại* đã cách ly.
- Trong hầu hết các trường hợp, bạn có thể xoá *phần mềm gián điệp* đã cách ly. *Phần mềm gián điệp* đã cách ly có thể là một phần của chương trình phần mềm hợp pháp và việc xoá đó sẽ ngăn chương trình thực tế hoạt động chính xác. Nếu bạn muốn giữ lại chương trình trên máy tính của mình, bạn có thể khôi phục *phần mềm gián điệp* đã cách ly.
- *Phần mềm nguy hiểm* đã cách ly có thể là một chương trình phần mềm hợp pháp. Nếu bạn đã tự cài đặt và thiết lập chương trình, bạn có thể khôi phục chương trình đó từ khu vực cách ly. Nếu *phần mềm nguy hiểm* được cài đặt mà bạn không biết, có thể nó được cài đặt với mục đích xấu và cần được xoá.

Xem các mục được cách ly

Bạn có thể xem thêm thông tin về các mục trong khu vực cách ly.

Để xem thông tin về các mục trong khu vực cách ly:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Bảo mật Máy tính** > **Quét vi-rút và phần mềm gián điệp**.
3. Nhấp vào **Xem mục cách ly**.
   Trang **Cách ly** hiển thị tổng số mục được lưu trữ trong khu vực cách ly.
4. Để xem thông tin chi tiết về các mục trong khu vực cách ly, hãy nhấp vào **Chi tiết**.

   Bạn có thể phân loại nội dung theo tên phần mềm độc hại hoặc đường dẫn tệp.

   Danh sách 100 mục đầu tiên được hiển thị với loại mục đã cách ly, tên của chúng và đường dẫn nơi các tệp được cài đặt.
5. Để xem thêm thông tin về mục đã cách ly, hãy nhấp vào biểu tượng bên cạnh mục trên cột **Trạng thái**.

Khôi phục mục đã cách ly

Bạn có thể khôi phục các mục đã cách ly mà bạn cần.

Bạn có thể khôi phục ứng dụng hoặc tệp từ khu vực cách ly nếu bạn cần chúng. Đừng khôi phục bất kỳ mục nào từ khu vực cách ly trừ khi bạn chắc chắn rằng chúng không mang lại nguy hiểm. Các mục được khôi phục chuyển trở lại vị trí bạn đầu trong máy tính của bạn.

Để khôi phục các mục đã cách ly:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Bảo mật Máy tính** > **Quét vi-rút và phần mềm gián điệp**.
3. Nhấp vào **Xem mục cách ly**.
4. Chọn mục đã cách ly mà bạn muốn khôi phục.
5. Nhấp vào **Khôi phục**.

DeepGuard là gì

DeepGuard phân tích nội dung của tệp và hành vi của ứng dụng và giám sát những ứng dụng không đáng tin cậy.

DeepGuard chặn *vi-rút*, *sâu* mới và chưa được phát hiện cũng như những ứng dụng độc hại khác cố thực hiện thay đổi đối với máy tính của bạn và ngăn các ứng dụng đáng ngờ truy cập vào Internet.

Khi DeepGuard phát hiện thấy ứng dụng mới cố thực hiện các thay đổi có thể gây hại đối với hệ thống, DeepGuard cho phép ứng dụng chạy trong khu vực an toàn. Trong khu vực an toàn, ứng dụng không thể gây hại cho máy tính của bạn. DeepGuard phân tích những thay đổi mà ứng dụng cố thực hiện, và dựa trên phân tích này, quyết định xem ứng dụng có thể là *phần mềm độc hại* hay không. Nếu ứng dụng có thể là *phần mềm độc hại*, DeepGuard sẽ chặn ứng dụng.

Các thay đổi hệ thống có thể có hại mà DeepGuard phát hiện bao gồm:

- thay đổi cài đặt hệ thống (registry của Windows),
- cố gắng tắt các chương trình hệ thống quan trọng, ví dụ: các chương trình bảo mật như sản phẩm này và
- tìm cách chỉnh sửa các tệp hệ thống quan trọng.

Bật hoặc tắt DeepGuard

Bật DeepGuard để ngăn các ứng dụng khả nghi thực hiện các thay đổi hệ thống có thể có hại trong máy tính của bạn.

Nếu bạn có Windows XP, hãy đảm bảo bạn đã cài đặt Gói Dịch vụ 2 trước khi bật DeepGuard.

Để bật hoặc tắt DeepGuard:

1. Trên trang chính, nhấp **Trạng thái**.
2. Nhấp vào **Thay đổi cài đặt trên trang này**.

   Ghi chú: Bạn cần quyền quản trị để tắt các tính năng bảo mật.

3. Bật hoặc tắt **DeepGuard**.
4. Nhấp vào **Đóng**.

Cho phép các ứng dụng mà DeepGuard đã chặn

Bạn có thể kiểm soát những ứng dụng mà DeepGuard cho phép và chặn.

Đôi khi DeepGuard có thể chặn không cho ứng dụng an toàn chạy, ngay cả khi bạn muốn sử dụng ứng dụng và biết rằng ứng dụng đó an toàn. Việc này xảy ra do ứng dụng cố thực hiện thay đổi hệ thống có thể có hại. Bạn cũng có thể vô tình chặn một ứng dụng khi cửa sổ bật lên của DeepGuard được hiển thị.

Để cho phép một ứng dụng mà DeepGuard đã chặn::

1. Trên trang chính, hãy nhấp vào **Công cụ**.
2. Nhấp vào **Ứng dụng**.
   Danh sách **Các ứng dụng được giám sát** được hiển thị.
3. Tìm ứng dụng bạn muốn cho phép.

   Ghi chú: Bạn có thể nhấp vào tiêu đề cột để phân loại danh sách. Ví dụ: nhấp vào cột **Quyền** để phân loại danh sách thành các nhóm được cho phép và bị từ chối.

4. Chọn **Cho phép** trong cột **Quyền**.
5. Nhấp vào **Đóng**.

DeepGuard cho phép ứng dụng thực hiện lại các thay đổi hệ thống.

Sử dụng DeepGuard ở chế độ tương thích

Để được bảo vệ tối đa, DeepGuard tạm thời sửa đổi các chương trình đang chạy. Một số chương trình không bị hỏng hoặc bị sửa đổi và có thể không tương thích với tính năng này. Ví dụ: các trò chơi trực tuyến với các công cụ chống lừa đảo kiểm tra rằng các trò chơi đó chưa bị sửa đổi theo bất kỳ cách nào khi được chạy. Trong những trường hợp này, bạn có thể bật chế độ tương thích.

Để bật chế độ tương thích:

1. Trên trang chính, nhấp **Cài đặt**.

   Ghi chú: Bạn cần quyền quản trị để thay đổi cài đặt.

2. Chọn **Bảo mật Máy tính** > **DeepGuard**.
3. Chọn **Sử dụng chế độ tương thích**.
4. Nhấp vào **OK**.

Tác vụ cần thực hiện với cảnh báo hành vi đáng ngờ

DeepGuard giám sát ứng dụng không đáng tin cậy. Nếu ứng dụng được giám sát cố truy cập vào Internet, cố thực hiện thay đổi đối với hệ thống của bạn hoặc thực hiện hành vi đáng ngờ, DeepGuard sẽ chặn ứng dụng đó.

Khi bạn đã chọn **Cảnh báo tôi về hành vi đáng ngờ** trong cài đặt DeepGuard, DeepGuard thông báo cho bạn khi DeepGuard phát hiện thấy ứng dụng có thể có hại hoặc khi bạn khởi động ứng dụng có danh tiếng không xác định.

Để quyết định điều bạn muốn thực hiện với ứng dụng mà DeepGuard đã chặn:

1. Nhấp vào **Chi tiết** để xem thêm thông tin về chương trình.
   Phần chi tiết trình bày cho bạn:
   - vị trí của ứng dụng,
   - danh tiếng của ứng dụng trong Mạng Bảo vệ theo Thời gian thực và
   - mức độ phổ biến của ứng dụng.
2. Quyết định liệu bạn có tin cậy vào ứng dụng mà DeepGuard đã chặn hay không:
   - Chọn **Tôi tin tưởng ứng dụng. Hãy để ứng dụng tiếp tục.** nếu bạn không muốn chặn ứng dụng.

     Ứng dụng có thể an toàn hơn nếu:
     - DeepGuard chặn ứng dụng là kết quả của những hành động bạn đã thực hiện,
     - bạn nhận ra ứng dụng hoặc
     - bạn nhận ứng dụng từ một nguồn tin cậy.
   - Chọn **Tôi không tin tưởng ứng dụng. Tiếp tục chặn ứng dụng này.** nếu bạn muốn tiếp tục chặn ứng dụng đó.

     Ứng dụng có thể không an toàn hơn nếu:
     - ứng dụng không phổ biến,
     - ứng dụng có danh tiếng không xác định hoặc
     - bạn không biết ứng dụng.
3. Nếu bạn muốn gửi các ứng dụng đáng ngờ để phân tích:
   a) Nhấp vào **Báo cáo ứng dụng đến F-Secure**.
   Sản phẩm hiển thị các điều kiện gửi.
   b) Nhấp vào **Chấp nhận** nếu bạn đồng ý với các điều kiện và muốn gửi mẫu.

   Chúng tôi khuyên bạn nên gửi mẫu khi:
   - DeepGuard chặn ứng dụng mà bạn biết là an hoàn hoặc
   - bạn nghi ngờ ứng dụng có thể là *phần mềm độc hại*.