bitdefender

ANTIVIRUS 2008

Hướng dẫn

BitDefender Antivirus 2008

Hướng dẫn

Xuất bản 2007.12.14

Văn bản Pháp lý


bitdefender

Mục lục

Giấy phép bản quyền và bảo hành

NẾU BẠN KHÔNG ĐỒNG Ý VỚI NHỮNG ĐIỀU KHOẢN VÀ ĐIỀU KIỆN NÀY THÌ HÃY ĐỪNG NÊN CÀI PHẦN MỀM. NẾU BẠN CHỌN "TÔI ĐỒNG Ý", "OK", "TIẾP THEO", "YES" HOẶC CÀI ĐẶT VÀ SỬ DỤNG PHẦN MỀM BẰNG BẤT CỨ PHƯƠNG PHÁP NÀO, VÔ HÌNH CHUNG BẠN BẮT BUỘC HOẶC ĐÃ HIỂU LÀ PHẢI CHẤP NHẬN MỌI ĐIỀU KIỆN CỦA BẢN THỎA THUẬN NÀY

Những điều kiện thoả thuận này bao trùm những Giải pháp và Dịch vụ của BitDefender cho người dùng cá nhân mà đã cung cấp bản quyền cho bạn, bao hàm những tài liệu liên quan và những cập nhật hay nâng cấp của phần mềm đã được bán cho bạn dưới hình thức bản quyền hoặc thoả thuận dịch vụ như đã được định nghĩa trong tài liệu và mọi sao chép của những điều này.

Hợp đồng cấp phép là một thoả thuận hợp pháp giữa bạn (một cá nhân hoặc tổ chức sử dụng cuối) và BitDefender để được sử dụng sản phẩm phần mềm BitDefender như nêu ở trên, bao gồm phần mềm máy tính và có thể bao gồm các môi trường kết hợp, các tài liệu được in và các tài liệu "trực tuyến" hoặc điện tử (sau đây gọi là "BitDefender"), tất cả các hạng mục này được bảo hộ bởi luật bản quyền Mỹ và luật bản quyền quốc tế và bảo vệ hiệp ước quốc tế. Bằng cách cài đặt, sao chép hoặc sử dụng BitDefender, bạn đồng ý ràng buộc với các điều khoản của hợp đồng. Nếu bạn không đồng ý với các điều khoản của hợp đồng này, không được cài đặt hoặc sử dụng BitDefender; tuy nhiên bạn có thể gửi trả về nơi mua để đòi hoàn trả đầy đủ khoản tiền đã mua trong vòng 30 ngày sau khi bạn mua. Có thể cần phải xác định việc mua hàng của bạn.

Nếu bạn không đồng ý với những điều kiện của thoả thuận, hãy đừng cài và sử dụng BitDefender.

Bản quyền BitDefender. BitDefender được bảo vệ bởi luật bản quyền và các hiệp ước quốc tế về bản quyền, cũng như là các luật pháp và hiệp ước khác về sở hữu trí tuệ. BitDefender được cấp phép và không được bán.

CẤP GIẤY PHÉP. BitDefender cấp cho bạn và chỉ riêng bạn giấy phép không độc quyền, không được chuyển nhượng và chỉ có thể sử dụng cho BitDefender.

ỨNG DỤNG PHẦN MỀM. Bạn có thể cài đặt và sử dụng BitDefender, trên bao nhiêu máy tính cá nhân mà bạn cần trong giới hạn của số máy tính ghi trên bản quyền mà bạn nhận được. Bạn có thể sao chép CD để cất giữ.

BẢN QUYỀN NGƯỜI DÙNG MÁY CÁ NHÂN. Bản quyền này áp dụng cho phần mềm BitDefender được cài đặt trên một máy tính duy nhất và không cung cấp cho việc sử dụng cho các dịch vụ mạng. Mỗi người dùng có thể cài trên máy cá nhân và có thể

sao chép lại để cất giữ trên một máy phụ. Số người dùng chính được ghi trên tờ bản quyền mà bạn nhận được.

ĐIỀU KHOẢN CỦA GIẤY PHÉP: Giấy phép được cấp bắt đầu vào ngày mà bạn cài đặt, sao chép hay sử dụng BitDefender lần đầu tiên và chỉ tiếp tục sử dụng trên máy tính mà BitDefender được cài đặt ban đầu.

HẾT HẠN. Sản phẩm sẽ dừng thực thi chức năng của nó ngay khi đăng ký hết hạn.

NÂNG CẤP. Nếu sản phẩm BitDefender được mang nhãn hiệu là nâng cấp, thì trước đó bạn phải được cấp phép để sử dụng một sản phẩm được xác định bởi BitDefender là hợp pháp để nâng cấp và sử dụng tiếp BitDefender. Một phần mềm BitDefender có nhãn hiệu nâng cấp sẽ thay thế hoặc/và bổ sung sản phẩm mà đã có trên cơ sở về tính hợp pháp của bạn để có thể nâng cấp. Bạn có thể sử dụng sản phẩm được nâng cấp theo các điều khoản của hợp đồng cấp phép này. Nếu BitDefender là một bản nâng cấp của một phần gói chương trình phần mềm mà bạn cấp phép như là một sản phẩm đơn lẻ, bạn có thể sử dụng và chuyển nhượng BitDefender như là một phần của gói sản phẩm đơn lẻ và không thể tách rời để sử dụng trên nhiều hơn một máy tính.

BẢN QUYỀN. Mọi quyền hạn, tư cách và quyền lợi đối với BitDefender và mọi bản quyền có liên quan đến BitDefender (bao gồm và không giới hạn các hình ảnh, ảnh chụp, biểu trưng bày, phần hoạt ảnh, video, audio, âm nhạc, văn bản kể cả chương trình ứng dụng nhỏ với một nhiệm vụ cụ thể được kết hợp trong/với BitDefender), các tài liệu in đính kèm và bản sao của BitDefender là thuộc sở hữu của BitDefender. BitDefender được bảo vệ bởi luật bản quyền và các điều khoản liên quan của hiệp ước quốc tế. Vì thế bạn phải coi BitDefender như là một tài liệu được cấp bản quyền ngoại trừ việc bạn có thể cài đặt BitDefender trên một máy tính đơn lẻ miễn là bạn phải giữ bản gốc chỉ cho các mục đích sao lại hoặc niêm cất. Bạn không thể sao chép các tài liệu in được đính kèm BitDefender. Bạn phải soạn thảo và bao gồm các thông báo về bản quyền trong một mẫu gốc các bản sao được thiết lập trong bất kể môi trường hoặc hình thức nào mà ở đó BitDefender tồn tại. Bạn không được phép cấp phép tiếp, cho thuê lại, bán hoặc cho thuê BitDefender. Bạn không được đảo lộn trình tự kỹ thuật, biên tập lại, tháo rời, tạo các công việc phát sinh, sửa đổi, dịch thuật hoặc ỉm cách phát hiện mã nguồn của BitDefender.

ĐIỀU KIỆN BẢO HÀNH. BitDefender bảo đảm rằng môi trường trong đó BitDefender được phân phối không bị sai hỏng trong thời gian 30 ngày kể từ ngày bàn giao BitDefender cho bạn. BitDefender là người duy nhất có thể và được quyền sửa chữa những sản phẩm được giao, trong phạm vi có thể, thay thế phương tiện bị hỏng nếu xảy ra hoặc hoàn trả lại tiền mà bạn đã thanh toán cho BitDefender. BitDefender không đảm bảo rằng BitDefender sẽ không bị gián đoạn hoặc không có lỗi hoặc các lỗi sẽ được hiệu chỉnh ngay lập tức. BitDefender không đảm bảo rằng BitDefender

sẽ đáp ứng mọi yêu cầu của bạn. BitDefender KHÔNG CHẤP NHẬN MỌI BẢO HÀNH KHÁC CHO BITDEFENDER, ĐƯỢC BIỂU ĐẠT HOẶC NGẦM ĐỊNH. BẢO HÀNH NÊU TRÊN LÀ RIÊNG BIỆT VÀ THAY THẾ CHO MỌI ĐIỀU KIỆN BẢO HÀNH KHÁC ĐƯỢC BIỂU ĐẠT HOẶC NGẦM ĐỊNH, BAO GỒM CÁC BẢO ĐẢM NGẦM ĐỊNH VỀ KHẢ NĂNG BÁN HÀNG, THÍCH HỢP CHO MỘT MỤC ĐÍCH ĐẶC BIỆT, HOẶC KHÔNG VI PHẠM. CHÍNH SÁCH BẢO HÀNH NÀY TẠO CHO BẠN CÁC QUYỀN LỢI HỢP PHÁP. BẠN CÓ THỂ CÓ CÁC QUYỀN LỢI KHÁC THAY ĐỔI TỪ QUỐC GIA NÀY SANG QUỐC GIA KHÁC.

NGOÀI NHỮNG ĐIỀU NÓI RÕ TRONG BẢN THOẢ THUẬN NÀY, BitDefender KHÔNG CHẤP NHẬN BẤT KỲ MỘT BẢO HÀNH NÀO KHÁC, RÕ RÀNG HAY NGỤ Ý, VỚI SỰ TÔN TRỌNG SẢN PHẨM, NÂNG CẤP, BẢO TRÌ HOẶC HỖ TRỢ LIÊN QUAN HAY NHỮNG TÀI LIỆU KHÁC (HỮU HÌNH HOẶC VÔ HÌNH) HOẶC NHỮNG DỊCH VỤ ĐƯỢC CUNG CẤP. BitDefender KHẲNG ĐỊNH TỪ NAY TỪ CHỐI MỌI BẢO ĐẢM VÀ ĐIỀU KIỆN LIÊN ĐỚI, BAO GỒM, NHƯNG KHÔNG CHỈ, NHỮNG BẢO HÀNH LIÊN ĐỚI ĐỐI VỚI NHỮNG NHÀ KINH DOANH, NHỮNG NHU CẦU CÁ NHÂN, TỔ CHỨC, CHỨC VỤ, CÓ HAY KHÔNG LIÊN QUAN, ĐỘ CHÍNH XÁC CỦA SỐ LIỆU, CHUẨN XÁC CỦA NỘI DUNG DỮ LIỆU, HỆ THỐNG TÍCH HỢP, SỰ BẤT KHẢ XÂM PHẠM KHI LỌC THÔNG TIN, NGƯNG SẢN PHẨM, HOẶC XOÁ NHỮNG PHẦN MỀM CỦA BÊN THỨ BA, GIÁN ĐIỆP, PHẦN MỀM QUẢNG CÁO, COOKIE, E-MAIL, TÀI LIỆU VĂN BẢN, QUẢNG CÁO HOẶC TƯƠNG TỰ, CHO DÙ NÓ CÓ THỂ ĐẾN TỪ CHÍNH THỂ, LUẬT PHÁP, TRUYỀN THÔNG, HẢI QUAN HAY KINH DOANH.

TỪ CHỐI CHẤP NHẬN THIỆT HẠI. Bất cứ người nào sử dụng, kiểm tra hoặc đánh giá BitDefender đều phải chịu mọi rủi ro đối với chất lượng và quá trình thực hiện của BitDefender. Trong mọi trường hợp, BitDefender không chịu trách nhiệm cho mọi tổn thất dưới mọi hình thức, bao gồm và không giới hạn các thiệt hại trực tiếp hoặc gián tiếp phát sinh ngoài việc sử dụng, thực hiện hoặc giao phần mềm BitDefender, thậm chí nếu BitDefender đã được thông báo về khả năng của các tổn thất đó. MỘT VÀI QUỐC GIA KHÔNG CHO PHÉP GIỚI HẠN HOẶC LOẠI TRỪ TRÁCH NHIỆM ĐỐI VỚI CÁC THIỆT HẠI NGẪU NHIÊN HOẶC CÁC THIỆT HẠI SAU NÀY, VÌ THẾ CÁC GIỚI HẠN HOẶC NGOẠI LỆ TRÊN KHÔNG ÁP DỤNG CHO BẠN. TRONG MỌI TRƯỜNG HỢP TRÁCH NHIỆM CỦA BitDefender SẼ KHÔNG VƯỢT QUÁ GIÁ MUA DO BẠN THANH TOÁN CHO SẢN PHẨM PHẦN MỀM BitDefender. Từ chối trách nhiệm và các giới hạn nêu trên sẽ được áp dụng bất kể bạn có chấp nhận hoặc sử dụng, đánh giá hoặc kiểm tra BitDefender hay không.

THÔNG BÁO QUAN TRỌNG CHO NGƯỜI DÙNG. THÔNG BÁO QUAN TRỌNG ĐỐI VỚI NHỮNG NGƯỜI SỬ DỤNG. PHẦN MỀM NÀY KHÔNG ĐA NĂNG ĐỂ CHỊU MỌI LỖI VÀ KHÔNG ĐƯỢC THIẾT KẾ ĐỂ SỬ DỤNG TRONG MỌI MÔI TRƯỜNG NGUY HIỂM CẦN THỰC HIỆN HOẶC ĐIỀU HÀNH AN TOÀN KHI CÓ LỖI. PHẦN

MỀM NÀY KHÔNG ĐỂ SỬ DỤNG TRONG CÁC HOẠT ĐỘNG CỦA NGÀNH HÀNG KHÔNG, CÁC PHƯƠNG TIỆN HẠT NHÂN HOẶC CÁC HỆ THỐNG TRUYỀN THÔNG, CÁC HỆ THỐNG VŨ KHÍ, CÁC HỆ THỐNG HỖ TRỢ NHÂN SINH TRỰC TIẾP HOẶC GIÁN TIẾP, KIỂM SOÁT KHÔNG LƯU HOẶC CÁC ỨNG DỤNG HAY CÀI ĐẶT MÀ LỖI CÓ THỂ DẪN ĐẾN TỬ VONG, THƯƠNG VONG NGHIÊM TRỌNG HOẶC THIỆT HẠI VỀ TÀI SẢN.

TỔNG QUAN. Thoả thuận này sẽ được chi phối bởi Luật pháp Romania và các qui định và hiệp ước về bản quyền quốc tế. Chỉ có những cơ quan luật pháp của Romania mới có quyền phân xử với những vấn đề mâu thuẫn xảy ra ngoài những điều kiện của Bản Thoả thuận này.

Giá cả, giá thành và phí sử dụng BitDefender có thể được thay đổi mà không cần phải báo trước cho bạn.

Trong trường hợp bất kỳ một điều khoản nào của bản Thoả thuận này không còn có giá trị, điều đó sẽ không ảnh hưởng đến tính hiệu lực của các điều khoản còn lại của bản thoả thuận.

BitDefender và biểu tượng của BitDefender là nhãn hiệu đã được đăng ký của BitDefender. Mọi nhãn hiệu khác là sở hữu của những người chủ sở hữu hợp pháp của chúng.

Bản quyền có thể bị huỷ ngay lập tức mà không cần phải báo trước nếu như bạn vi phạm bất kỳ điều kiện nào trong bản này. Bạn cũng sẽ không nhận được bất cứ tiền trả lại nào từ BitDefender hoặc những nhà phân phối BitDefender về việc này. Những điều kiện liên quan đến việc bảo tín và hạn chế sử dụng vẫn còn hiệu lực kể cả sau khi cắt bản quyền.

BitDefender có thể xem xét lại những Điều kiện này bất cứ lúc nào và những thay đổi này sẽ được áp dụng ngay lập tức để phù hợp với từng phiên bản phần mềm được phân phối để phù hợp với những điều kiện thực tiễn mới. Nếu bất kỳ điểm nào trong thoả thuận này được bỏ qua và mất hiệu lực, nó sẽ không còn giá trị còn những điều còn lại khác vẫn còn giá trị và có hiệu lực.

Trong trường hợp không tương đồng giữa bản dịch của bản Thoả thuận này sang tiếng khác, bản Tiếng Anh được BitDefender cung cấp là bản chiếm ưu thế.

Liên hệ với BitDefender, Số 5 đường Fabrica de Glucoza 72322-Sector 2, Bucharest, Romania,hoặc bằng điện thoại: 40-21-2330780 hoặc Fax:40-21-2330763, địa chỉ e-mail: office@bitdefender.com. Và địa chỉ e-mail đại diện tại Việt Nam: sales@bitdefender.com.vn.

Lời nói đầu

Sách hướng dẫn này dành cho tất cả những người sử dụng đã lựa chọn **BitDefender Antivirus 2008** như là một giải pháp an ninh cho các máy tính cá nhân của họ. Các thông tin thể hiện trong cuốn sách này là thích hợp không những đối với những người thông hiểu về máy tính, mà còn thích hợp với mọi người có khả năng làm việc trong môi trường Windows và có thể truy cập được.

Cuốn sách này miêu tả **BitDefender Antivirus 2008**, công ty và nhóm thiết kế đã xây dựng lên phần mềm này sẽ hướng dẫn bạn trong suốt quá trình cài đặt, hướng dẫn bạn cách lập cấu hình cho phần mềm. Bạn sẽ nhận biết cách sử dụng **BitDefender Antivirus 2008**, cập nhật, kiểm tra và cá nhân hoá phần mềm. Bạn sẽ biết được những điều tốt nhất từ BitDefender.

Chúng tôi chúc bạn có một bài giảng hữu ích và lý thú.

1. Các qui ước sử dụng trong cuốn sách này

1.1. Các qui ước về nghệ thuật in

Một vài thể loại văn bản được sử dụng trong cuốn sách để nâng cao khả năng dễ đọc. Phạm vi và ý nghĩa của các thể loại này được thể hiện trong bảng dưới đây.

Thể hiện	Miêu tả
`sample syntax`	Các mẫu cú pháp được in với các `ký tự cách đơn`.
http://www.bitdefender.com	Các liên kết URL đang chỉ tới một số vị trí bên ngoài, trên các máy chủ http hoặc ftp
support@bitdefender.com	Các thông điệp email được chèn vào văn bản để thông báo về các địa chỉ liên hệ.
“Lời nói đầu” (p. xi)	Đây là một liên kết bên trong, hướng về một số vị trí bên trong văn bản.
`filename`	Tệp và thư mục được in sử dụng các font `chữ đơn cách`.

Thể hiện	Miêu tả
option	Tất cả các lựa chọn sản phẩm được in sử dụng các ký tự **mạnh**.
`sample code listing`	In mã với các `ký tự đơn cách.`

1.2. Lời nhắc nhở

Những lời nhắc nhở là các thông báo bằng văn bản, được biểu thị sinh động, thu hút sự chú ý của bạn với các thông tin bổ sung có liên quan đến đoạn hiện tại.

Ghi chú

Thông báo chỉ là một quan sát ngắn. Mặc dù bạn có thể bỏ qua nhưng những thông báo này vẫn có thể cung cấp những thông tin có giá trị như một đặc điểm cụ thể hoặc một mối liên hệ với một đề tài có liên quan nào đó.

Quan trọng

Phần này đòi hỏi bạn phải chú ý, bạn không nên bỏ qua. Thông thường, nó cung cấp những thông tin không phải là quan trọng nhưng cũng đáng để xem xét.

Cảnh báo

Đây là thông tin quan trọng mà bạn cần xử lý với sự chú ý cao. Sẽ không có gì xấu xảy ra nếu bạn làm theo các chỉ dẫn. Bạn cần đọc và hiểu nó bởi vì nó mô tả một vấn đề gì đó chứa nguy cơ rất cao.

2. Cấu trúc của cuốn sách

Sách gồm có nhiều phần chứa đựng những đề tài chính. Ngoài ra , một bảng chú giải được cung cấp với cách trình bày một cách dễ hiểu với những kiến thức chuyên môn

Các bước cài đặt. Các chỉ dẫn từng bước để cài đặt BitDefender vào trạm công tác. Đây là hướng dẫn toàn diện về cách cài đặt **BitDefender Antivirus 2008**. Bắt đầu bằng những điều kiện tiên quyết để cài đặt thành công, bạn sẽ được chỉ dẫn trong suốt quá trình cài đặt. Cuối cùng thủ tục dỡ bỏ được miêu tả trong trường hợp bạn bạn cần phải dỡ bỏ phần cài đặt BitDefender.

Quản lý cơ bản. Mô tả cơ bản về quyền quản trị và sự bảo trì của BitDefender.

Quản lý an ninh cấp cao. Một bản trình bài chi tiết về những khả năng bảo mật được phân phối bởi BitDefender. Giải thích một cách chi tiết tất cả những vấn đề về

những tùy chọn và tinh chỉnh nâng cao. Bạn được chỉ dẫn làm thế nào để cấu hình và sử dụng mọi mô-đun chức năng của Bitdefender nhằm bảo vệ có hiệu quả máy tính của bạn khỏi các hiểm họa như viruses, spyware, rootkits...

Đĩa CD Hồi phục BitDfender. Miêu tả đĩa CD Hồi phục BitDefender. Nó giúp hiểu và nắm cách sử dụng các đặc điểm do đĩa CD này cung cấp.

Nhận trợ giúp. Xem và yêu cầu trợ giúp ở đâu khi có gì bất bình thường xuất hiện.

Sổ tay thuật ngữ. Cuốn sổ này giải thích các thuật ngữ kỹ thuật và không thông dụng mà bạn gặp phải ở các trang trong tài liệu này.

3. Xin ý kiến đóng góp

Xin bạn hãy giúp chúng tôi cải thiện cuốn sách này. Chúng tôi đã thử nghiệm và xác minh tất cả các thông tin trong khả năng của mình. Xin hãy gửi thư và cho chúng tôi biết các thiếu sót bạn phát hiện được trong cuốn sách này và theo bạn, làm cách nào để cải thiện chúng để chúng tôi có thể cung cấp cho bạn cuốn sách tốt nhất có thể.

Cho chúng tôi biết bằng cách gửi e-mail đến documentation@bitdefender.com.

Quan trọng

Xin hãy viết tất cả các thư từ liên quan đến tài liệu bằng tiếng Anh để chúng tôi có thể xử lý chúng một cách có hiệu quả.

Các bước cài đặt

1. Cài đặt BitDefender Antivirus 2008

Phần **BitDefender Antivirus 2008 Cài đặt** của hướng dẫn sử dụng này bao gồm những đề tài sau:

- Các yêu cầu về hệ thống
- Các bước Cài đặt
- Thuật sĩ cài đặt
- Nâng cấp
- Gỡ bỏ hoặc sửa chữa hoặc thay đổi các chức năng của BitDefender

1.1. Các yêu cầu của Hệ thống

Để đảm bảo cho sản phẩm hoạt động tốt, trước khi lắp đặt cần xác nhận rằng những đòi hỏi về hệ thống sau đây phải được đáp ứng:

- Hoạt động tốt trên: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (hoặc cao hơn)

Windows 2000/XP

- Vi xử lý 800MHz hoặc cao hơn
- Bộ nhớ RAM tối thiểu là 256 MB (khuyến cáo nên sử dụng 512 MB)
- Đĩa cứng phải có dung lượng tối thiểu là 60 MB

Windows 2000/XP

- Vi xử lý 800MHz hoặc cao hơn
- Bộ nhớ RAM tối thiểu là 256 MB (khuyến cáo nên sử dụng 1 GB)
- Đĩa cứng phải có dung lượng tối thiểu là 60 MB

Windows Vista

- Vi xử lý 800MHz hoặc cao hơn
- Bộ nhớ RAM tối thiểu là 512 MB (khuyến cáo nên sử dụng 1 GB)
- Đĩa cứng phải có dung lượng tối thiểu là 60 MB

BitDefender Antivirus 2008 có thể tải về để đánh giá từ http://www.bitdefender.com.

1.2. Các bước cài đặt

Định vị file cài đặt và nhấn đúp chuột. Sẽ có cẩm nang hướng dẫn bạn trong suốt quá trình cài đặt

Trước khi kích hoạt thuật sĩ cài đặt, BitDefender sẽ kiểm tra phiên bản mới nhất với gói cài đặt. Nếu có phiên bản mới nhất thời điểm đó, bạn sẽ được nhắc nhở để tải xuống nó. Click **Yes** để tải xuống phiên bản mới nhất hoặc **No** để tiếp tục cài đặt với phiên bản hiện tại.

Các bước cài đặt

Tiến hành theo những bước này để cài đặt BitDenfender Antivirus 2008:

1. Nhấp chuột vào **Tiếp theo** để tiếp tục hoặc nhấp vào **Huỷ bỏ** nếu bạn muốn thoát khỏi chương trình cài đặt.
2. Nhấp chuột vào **Next**.

BitDefender Antivirus 2008 sẽ cảnh báo cho bạn nếu có các sản phẩm chống virus khác được cài đặt trong máy tính của bạn. **Remove** - để dỡ bỏ tất cả các phần đã được cài đặt. Nếu bạn muốn tiếp tục cài đjặt mà không xóa phiên bản cũ, bấm **Next**.

Cảnh báo

Xin khuyến cáo rằng tốt nhất bạn không nên cài đặt bất cứ chương trình tìm và diệt virus nào khác trước khi cài đặt BitDefender. Chạy hai hoặc nhiều hơn chương trình diệt virus cùng một lúc sẽ làm cho hệ thống không thể sử dụng được.

3. Xin hãy đọc Thoả thuận cấp phép, chọn **Tôi chấp nhận các điều khoản trong thoả thuận** và nhấp vào **Sau đó**. Nếu bạn không đồng ý với các điều khoản này, hãy nhấp vào **Huỷ bỏ**. Quá trình cài đặt sẽ chấm dứt và bạn có thể thoát khỏi chương trình cài đặt.
4. Theo thiết lập mặc định, BitDefender Antivirus 2008 sẽ được cài đặt vào `C:\Program Files\BitDefender\BitDefender 2008`. Nếu bạn muốn chọn thư mục khác nhấp chuột vào **Browse** và trên cửa sổ mở, hãy chọn thư mục mà bạn muốn cài đặt BitDefender Antivirus 2008. Nhấp vào **Tiếp theo**.

   Nhấp chuột vào **Next**.
5. Hãy chọn những tùy chọn đối với tiến trình cài đặt Bạn có hai phương án lựa chọn mặc định:
   - **Mở readme file** - để mở tập tin readme vào thời điểm cuối khi lắp đặt.
   - **" Đặt một đường tắt trên màn hình nền** - Để đặt đường tắt cho BitDefender Antivirus 2008 trên màn hình nền của bạn vào cuối thời gian cài đặt.
   - **Eject CD when installation is complete** - để lấy CD ra khi kết thúc quá trình cài đặt; tùy chọn này sẽ xuất hiện khi bạn cài đặt sản phẩm từ CD.
   - **Turn off Windows Defender** - để tắt Windows Defender; tùy chọn này sẽ chỉ xuất hiện trong Windows Vista.

   Nhấp vào **Cài đặt** để bắt đầu cài đặt sản phẩm.

Quan trọng

Trong quá trình cài đặt sẽ có một wizard xuất hiện. Thuật sĩ này sẽ giúp bạn đăng ký **BitDefender Antivirus 2008**, tạo ra một tài khoản BitDefender và lắp đặt BitDefender để thực hiện các tác vụ an ninh quan trọng.
Hãy hoàn tất quá trình được cẩm nang hướng dẫn để chuyển sang các bước tiếp theo.

6. Nhấp vào **Kết thúc**. Bạn có thể được yêu cầu khởi động lại hệ thống để wizard cài đặt có thể hoàn tất quá trình cài đặt. Chúng tôi khuyên bạn nên làm như vậy càng sớm càng tốt.

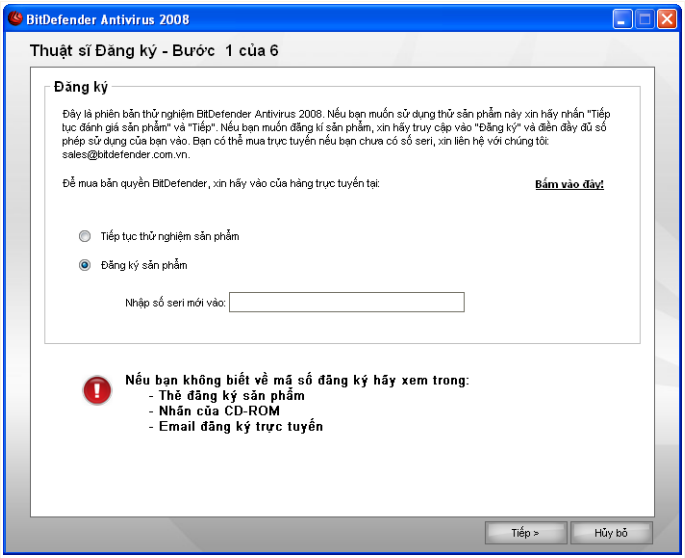
Nếu bạn chấp nhận cài đặt mặc định thì một thư mục có tên gọi là `BitDefender` được tạo ra trong `Program Files` và nó chứa đựng thư mục phụ `BitDefender 2008`.

1.3. Wizard cài đặt đầu tiên

Trong quá trình cài đặt, một wizard sẽ xuất hiện. Wizard này giúp bạn đăng ký **BitDefender Antivirus 2008**, tạo ra một tài khoản BitDefender và giao cho BitDefender thực hiện các nhiệm vụ an ninh quan trọng.

Không bắt buộc phải kết thúc wizard này song chúng tôi khuyến cáo bạn nên làm như vậy để tiết kiệm thời gian và đảm bảo cho hệ thống của bạn an toàn thậm chí là trước khi BitDefender Antivirus 2008 được cài đặt.

1.3.1. Bước 1/6 - Đăng ký BitDefender Antivirus 2008



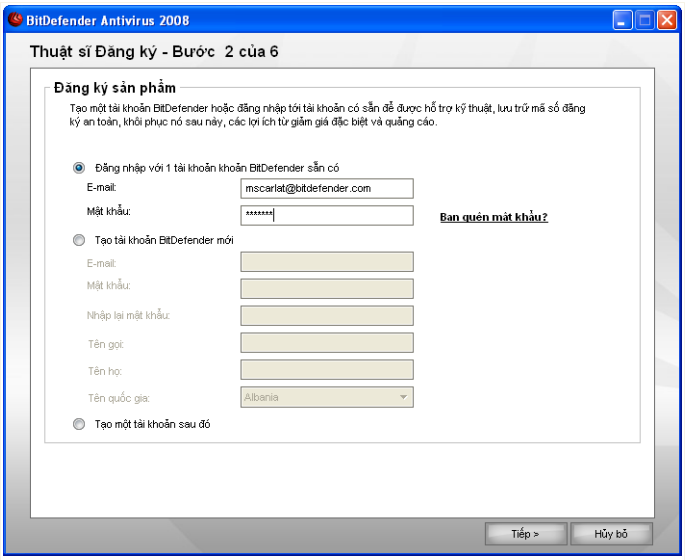
Đăng ký

Chọn **Đăng ký sản phẩm**để đăng ký **BitDefender Antivirus 2008**. Đánh chìa khoá của giấy phép vào **Enter new key** field.

Để tiếp tục đánh giá sản phẩm, chọn**Tiếp tục đánh giá sản phẩm**.

Nhấp chuột vào **Next**.

1.3.2. Bước 2/6 - Tạo một tài khoản BitDefender



Thiết lập tài khoản

Tôi không có tài khoản BitDefender

Để hưởng hỗ trợ kỹ thuật miễn phí của BitDefender và các dịch vụ miễn phí khác bạn phải thiết lập một tài khoản. Chọn **Mở tài khoản BitDefender của tôi** để tạo tài khoản BitDefender của bạn. Cần nối mạng Internet. Các dữ liệu bạn đã cung cấp sẽ được giữ bí mật.

Ghi chú
Nếu bạn muốn tạo tài khoản sau , hãy chọn tùy chọn tương ứng.

Đánh địa chỉ email đang còn hiệu lực vào **E-mail** field. Nhớ mật khẩu và gõ vào **Password** field. Khẳng định mật mã vào **Đánh lại mật mã** field. Sử dụng mật mã và địa chỉ email để nối vào tài khoản của bạn ởhttp://myaccount.bitdefender.com.

Ghi chú

Mật khẩu phải có ít nhất bốn ký tự.

Điền họ và tên của bạn và chọn tên đất nước bạn đang cư trú.

Đê thiết lập thành công một tài khoản, đầu tiên bạn phải kích hoạt địa chỉ email của bạn. Kiểm tra địa chỉ email của bạn và làm theo các chỉ dẫn trong email do dịch vụ đăng ký BitDefender gửi đến cho bạn.

Click **Tiếp** để đi tiếp hoặc **Thoát** để ra khỏi wizard.

Tôi đã có tài khoản BitDefender

Nếu bạn đã có TK còn giá trị, chọn **Truy cập tài khoản BitDefender đang có** và hãy vào địa chỉ email và mật khẩu TK của bạn.

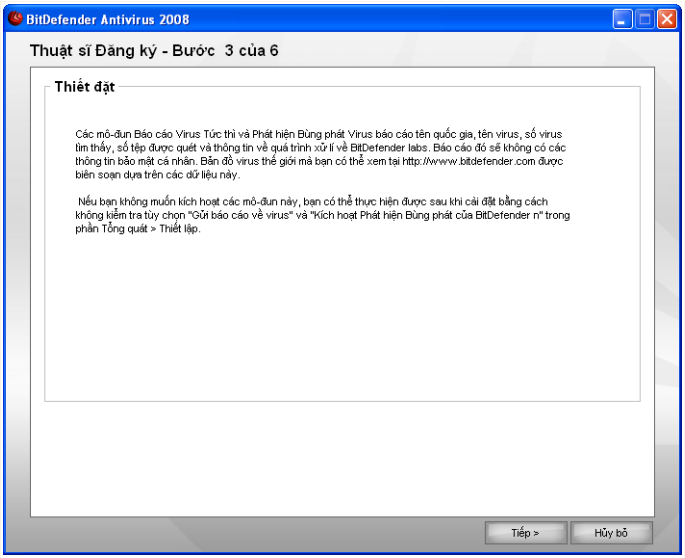
Ghi chú

Nếu bạn vào sai mật khẩu, bạn sẽ được nhắc và vào lại 2 lần khi nhấn **Tiếp**. Click **OK** để vào lại mật khẩu hoặc **Cancel** để ra khỏi wizard.

Nếu bạn quên mật khẩu, nhấp **Bạn quên mật khẩu?** và làm theo các hướng dẫn.

Click **Tiếp** để đi tiếp hoặc **Thoát** để ra khỏi wizard.

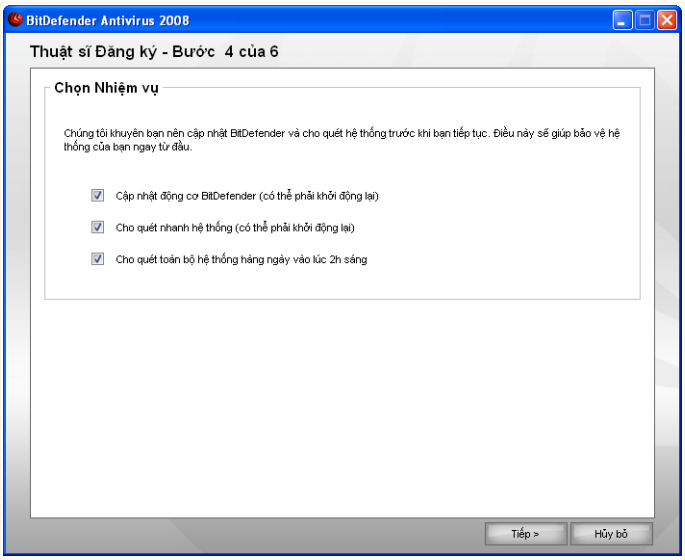
1.3.3. Bước 3/6 - Các thông tin về virus theo thời gian thực RTVR



Các thông tin về RTVR

Click **Tiếp** để đi tiếp hoặc **Thoát** để ra khỏi wizard.

1.3.4. Bước 4/6 - Chọn tác vụ cần thực hiện



Chọn Nhiệm vụ

Giao cho BitDefender Antivirus 2008 thực hiện các nhiệm vụ quan trọng là đảm bảo an ninh cho hệ thống cuả bạn.

Có những lựa chọn sau:

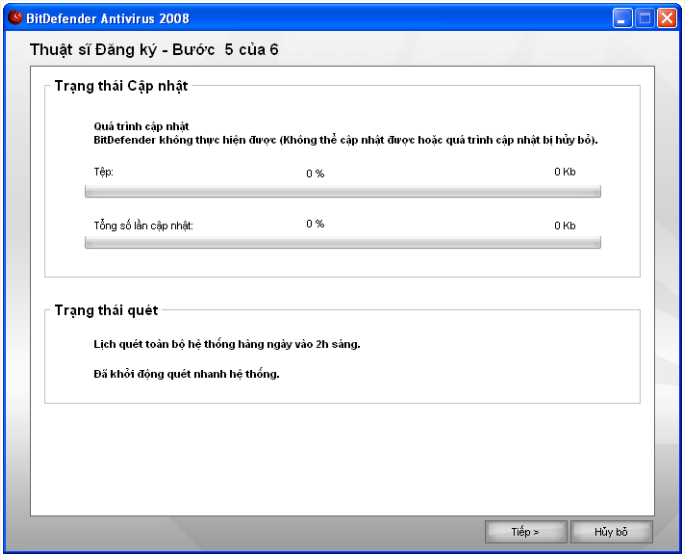
- **Nâng cấp BitDefender engines (có thể cần phải khởi động lại)** - Trong bước tiếp theo, một hoạt động nâng cấp BitDefender engines sẽ được thực hiện để bảo vệ máy tính của bạn khỏi những mối đe doạ mới nhất.
- **Quét nhanh hệ thống (có thể cần phải khởi động lại)** - trong bước tiếp theo, một động tác quét nhanh hệ thống sẽ được vận hành để sao cho BitDefender có thể đảm bảo rằng các tập tin của bạn từ các thư mục`Windows` and `Program Files`không bị nhiễm virus.
- **Vận hành việc quét toàn bộ hệ thống hàng ngày vào lúc 2 giờ sáng** - Vận hành việc quét toàn bộ hệ thống hàng ngày vào lúc 2 giờ sáng.

Quan trọng
Chúng tôi khuyến cáo bạn nên tạo khả năng cho các phương án này, trước khi chuyển sang bước tiếp theo để đảm bảo an toàn cho hệ thống của bạn.

Nếu bạn chỉ chọn giải pháp cuối cùng hoặc không chọn giải pháp nào cả, bạn sẽ bỏ qua bước tiếp theo.

Click **Tiếp** để đi tiếp hoặc **Thoát** để ra khỏi wizard.

1.3.5. Bước 5/6 - Hãy đợi để các tác vụ được hoàn tất

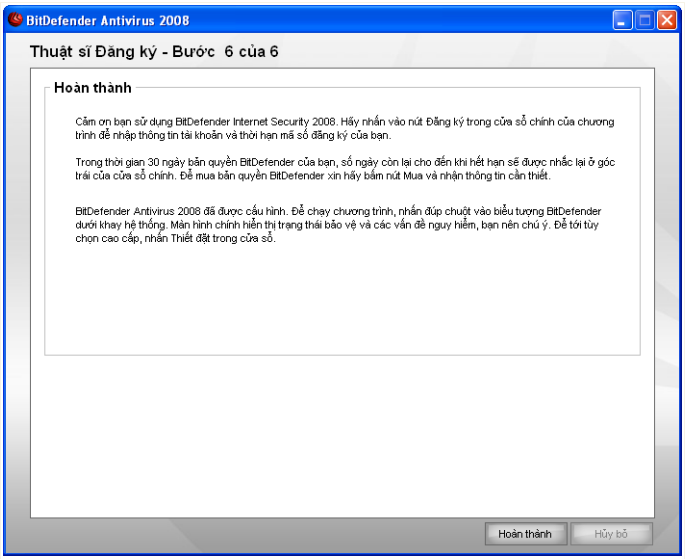


Tình trạng nhiệm vụ

Hãy đợi nhiệm vụ hoàn tất. Bạn có thể thấy được tình trạng nhiệm vụ (các nhiệm vụ) được chọn ở bước trước đó.

Click **Tiếp** để đi tiếp hoặc **Thoát** để ra khỏi wizard.

1.3.6. Bước 6/6 - Tóm tắt thông tin



Kết thúc

Đây là bước cuối cùng của wizard cấu hình.

Nhấp **Finish** để hoàn tất wizard và tiếp tục quá trình cài đặt.

1.4. Nâng cấp

Thủ tục nâng cấp có thể được thực hiện bằng một trong các cách sau đây:

- **cài đặt không cần dỡ bỏ phiên bản trước đây- đối với v8 hoặc cao hơn, loại trừ Internet Security**

  Nhấp đúp thư mục cài đặt và theo chỉ dẫn (wizard) tại phần “*Các bước cài đặt*” (p. 3).

Quan trọng

Trong quá trình cài đặt, một thông điệp lỗi do `dịch vụ Filespy` , sẽ xuất hiện. Nhấp **OK** để tiếp tục cài đặt.

- **Không lắp đặt phiên bản trước đây mà lắp đặt phiên bản mới - cho tất cả các phiên bản BitDefender**

  Đầu tiên, bạn cần dỡ bỏ phiên bản trước đây, sau đó khởi động lại máy tính và cài đặt phiên bản mới như được mô tả trong phần "*Các bước cài đặt*" (p. 3).

Quan trọng

Nếu bạn nâng cấp từ BitDefender v8 hoặc cao hơn, chúng tôi khuyến cáo bạn nên lưu lại BitDefender settings. Sau khi kết thúc quá trình nâng cấp, bạn có thể tải chúng xuống.

1.5. Gỡ bỏ, sửa chữa và thay đổi các chức năng của BitDefender

Nếu bạn muốn thay đổi, sửa chữa hoặc gỡ bỏ **BitDefender Antivirus 2008**, bạn hãy theo đường dẫn từ thực đơn khởi động của Windows **Start** → **Programs** → **BitDefender 2008** → **Thay đổi, Sửa chữa và Không cài đặt** .

Bạn có thể được yêu cầu khẳng định sự lựa chọn của bạn bằng cách nhấp chuột vào **Next**. Một cửa sổ mới sẽ xuất hiện để bạn có thể lựa chọn:

- **Sửa chữa** - để cài đặt lại tất cả các phần của chương trình đã được cài đặt trước đó;

  Quan trọng

  Trước khi sửa chữa sản phẩm, chúng tôi khuyến cáo bạn nên lưu lại Sổ Trắng và Sổ Đen. Bạn cũng nên lưu lại Thiết lập của Bitdefender và cơ sở dữ liệu Bayesian. Sau khi quá trình sửa chữa kết thúc bạn có thể nạp lại chúng.

  Nếu bạn muốn chọn để sửa Bitdefender, cửa sổ tiếp theo sẽ xuất hiện: Nhấp **Repair** để bắt đầu quá trình.

  Khởi động lại máy tính khi được nhắc nhở và sau đó click **Install** để cài đặt lại BitDefender Antivirus 2008.

  Một khi tiến trình cài đặt hoàn tất, một cửa sổ mới sẽ xuất hiện. Nhấp vào **Kết thúc**.
- **Remove** - để dỡ bỏ tất cả các phần đã được cài đặt.

Ghi chú

Chúng tôi khuyến cáo bạn nên chọn **Remove** - để dỡ bỏ tất cả các phần đã được cài đặt.

Nếu bạn chọn xóa bỏ Bitdefender, cửa sổ tiếp theo sẽ xuất hiện.

Quan trọng

Khi gỡ bỏ BitDenfender , bạn sẽ không còn được bảo vệ để chống lại sự đe dọa của malware cũng như virus và spyware. Nếu bạn muốn Windows Defender được kích hoạt sau khi gỡ bỏ BitDefender, hãy đánh dấu kiểm vào hộp tương ứng. Đây là tùy chọn chỉ có hiệu lực trong Windows Vista

Nhấp **Remove**để bắt đầu xóa bỏ BitDefender Antivirus 2008 khỏi máy tính của bạn.

Trong suốt quá trình xóa bỏ bạn sẽ được nhắc nhở gửi cho chúng tôi những phản hồi của bạn. Nhấp **OK**để tham gia vào khảo sát trực tuyến. Nếu bạn không muốn tham gia khảo sát, hãy bấm nút **Cancel**.

Một khi tiến trình xóa bỏ hoàn tất, một cửa sổ mới sẽ xuất hiện. Nhấp vào **Kết thúc**.

Ghi chú

Sau khi quá trình xóa bỏ hoàn tất, chúng tôi khuyến cáo bạn nên xóa thư mục `BitDefender` ở `Program Files`.

Lỗi khi xóa bỏ Bitdefender

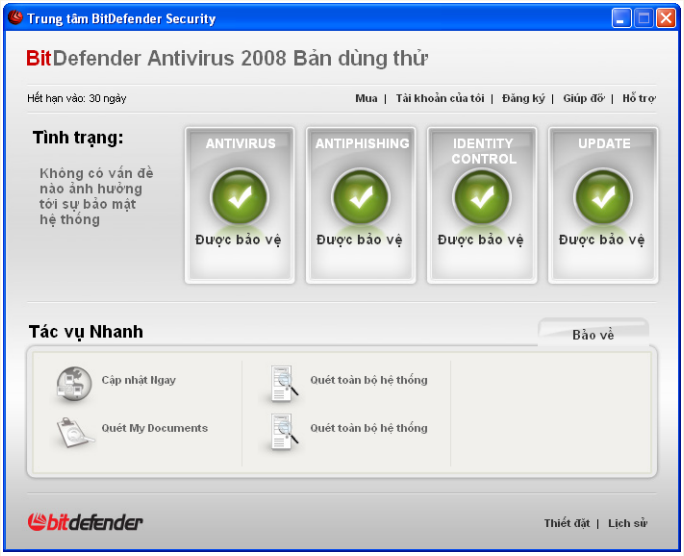
Nếu có lỗi trong quá trình di dời của BitDefender, tiến trình xóa bỏ sẽ bị hủy và một cửa sổ mới sẽ xuất hiện. Nhấp **Run UninstallTool** để chắc chắn rằng Bitdefender đã được xóa bỏ hoàn toàn. Công cụ xóa bỏ sẽ di chuyển tất cả những File và khóa của Registry mà chưa được xóa bỏ trong suốt quá quá trình tự động xóa bỏ.

Quản lý cơ bản

2. Bắt đầu

Một khi bạn đã cài đặt BitDefender thì máy tính của bạn đã được bảo vệ. Bạn có thể mở BitDefender Security Center để kiểm tra mức độ an ninh của hệ thống, đánh giá những mối nguy hiểm hoặc tinh chỉnh toàn bộ sản phẩm bất cứ lúc nào.

Để truy cập BitDefender Security Center ,sử dụng thực đơn Start của Windows, bằng cách theo đường dẫn **Start → Programs → BitDefender 2008 → BitDefender Antivirus 2008** hoặc để nhanh hơn nhấp đúp vào **BitDefender icon** từ ngăn hệ thống.



BitDefender Security Center

Trung tâm an toàn BitDefender gồm có 2 vùng:

- **Khu vực trạng thái**: bao gồm thông tin về chương trình và trợ giúp bạn sửa các lỗi bảo mật có thể bị tấn công trên máy tính của bạn. Bạn có thể dễ dàng nhận ra ngay công dụng của nó tác động đến máy tính của bạn. Bằng cách ấn vào nút mầu đỏ**Giải quyết mọi đối tượng** mọi điểm yếu trên máy tính sẽ được giải quyết ngay

lập tức hoặc bạn sẽ được hướng dẫn sửa chữa một cách dễ dàng. Cùng một thời điểm, có bốn nút trạng thái được kích hoạt tương ứng với bốn danh mục bảo mật. Nút trạng thái mầu Xanh cho ta biết không có bất cứ nguy hiểm nào. Nút mầu Vàng hoặc Đỏ cho biết lỗi bảo mật ở mức độ Trung bình hoặc Cao. Để sửa các vấn đề đó, ấn vào nút mầu Vàng/Đỏ, khi đó nút **Sửa lỗi** để sửa từng lỗi một hoặc nút **Giải quyết tất ngay**. Nút mầu xám cho biết một thành phần chưa được thiết lập.

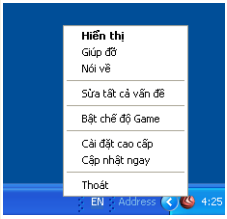
- The **Quick Tasks** area: helps you keep your system safe and protect your data.

Hơn thế nữa, BitDefender Security Center bao gồm những biểu tượng rất hữu ích.

Liên kết	*Miêu tả*
Mua	Mở một trang web nơi mà bạn có thể mua sản phẩm.
My Account	Mở trang tài khoản Bitdefender của bạn.
Register	Mở thuật sĩ đăng ký.
Help	Mở File trợ giúp.
Support	Mở trang web hỗ trợ của BitDenfender.
Thiết lập	Mở tinh chỉnh nâng cao.
History	Mở một cửa số với các sự kiện & lịch sử của BitDefender

2.1. Biểu tượng BitDefender trong System Tray

Để quản lí toàn bộ sản phẩm nhanh hơn , bạn có thể sử dụng biểu tượng của BitDefender ở khay hệ thống.



Trình đơn ngữ cảnh

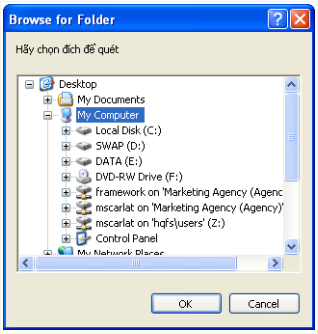
Nếu bạn nhấp đúp biểu tượng này, console quản lý sẽ mở ra. Nếu nhấp chuột phải,trình đơn ngữ cảnh sẽ mở ra. Nó giúp quản lý nhanh BitDefender:

- **Show** - mở BitDefender Security Center.
- **Help** - Mở tập tin trợ giúp.
- **About** -mở trang web Bitdefender.
- **Fix all issues** - giúp bạn xử lý những lỗi bảo mật hiện tại.
- **Bật /tắt chế độ game** - Bật / tắt Game Mode.
- **Open advanced settings** - cho phép bạn truy cập tinh chỉnh cao cấp.
- **Cập nhật ngay** - hãy tiến hành cập nhật ngay. Một cửa sổ mới sẽ xuất hiện, nơi bạn có thể xem tình trạng cập nhật.
- **Exit** - đóng ứng dụng.

2.2. BitDefender quét thủ công

Nếu bạn chắc chắn muốn quét nhanh một thư mục , bạn có thể sử dụng BitDefender Manual Scan.

Để chạy BitDefender Manual Scan, sử dụng trình đơn Start của Windows, bằng cách dùng đường dẫ sau **Start → Programs → BitDefender 2008 → BitDefender Manual Scan** Cửa sổ kế tiếp hiện ra:



BitDefender quét thủ công

Tất cả những gì bạn phải làm là chọn thư mục muốn quét, và bấm **OK**. Bộ quét BitDefender sẽ hiện lên và dẫn bạn đến quy trình quét.

2.3. Chế độ Game

Chế độ Game mới tạm thời thay đổi Cấu hình an ninh để giảm thiểu sự ảnh hưởng đến game mà vẫn giữ an toàn và chơi thoải mái. Khi bạn kích hoạt chế độ Game, những cấu hình sau sẽ được áp dụng:

- Tất cả các cảnh báo và pop-up BitDefender đều bị ngừng.
- Áp dụng mức độ bảo vệ thời gian thực ở mức **Cho phép**.

2.3.1. Dùng Chế độ Game

Nếu bạn muốn kích hoạt chế độ Game, hãy dùng một trong những phương pháp sau đây:

- Nhấp chuột phải vào biểu tượng BitDefender trong system tray và chọn **Khởi động Chế độ Game**.
- Nhấn `Alt+G` (phím tắt).

Quan trọng
Đừng quên tắt Chế độ Game đi khi xong. Bạn hãy dùng cùng phương pháp khi bật lên.

2.3.2. Thay đổi phím tắt Chế độ game

Để thay đổi phím tắt, làm theo các bước sau:

1. Click **Cấu hình** trong BitDefender Security Center để mở thanh cấu hình.

   Ghi chú
   Nhấp chuột phải vào biểu tượng BitDefender trong system tray và chọn **Mở cấu hình cao cấp**.

2. Click **Cao cấp**.
3. Dưới lựa chọn **Kích hoạt phím tắt Chế độ Game**, cài đặt phím tắt:
   - Chọn thay đổi phím mà bạn muốn dùng bằng cách tích một trong những: Phím (`Ctrl`), Phím (`Shift`) hoặc phím (`Alt`).
   - Trong trường sửa, gõ chữ tương ứng với phím mà bạn muốn dùng.

Ví dụ, bạn muốn dùng phím nóng `Ctrl+Alt+D` bạn phải chọn mỗi `Ctrl`, rồi `Alt` và `D`.

Ghi chú

Bỏ tích tiếp tới **Kích hoạt phím nóng Chế độ Game** sẽ ngưng phím nóng.

3. Tình trạng an ninh

Thanh tình trạng an nhin hiển thị tình trạng an ninh của hệ thống và dễ dàng quản lí danh sách những lỗ hổng bảo mật ở máy tính của bạn. BitDefender Antivirus 2008 sẽ cho bạn biết bất cứ lúc nào một vấn đề có thể làm ảnh hưởng đến mức độ an toàn của máy tính.

Có 4 biểu tượng tình trạng an ninh:

- **ANTIVIRUS**
- **ANTIPHISING**
- **KIỂM SOÁT TT CÁ NHÂN**
- **UPDATE**

At the same time, on the left you can see the number of issues affecting the security of your system and a red **Fix All Issues** button.

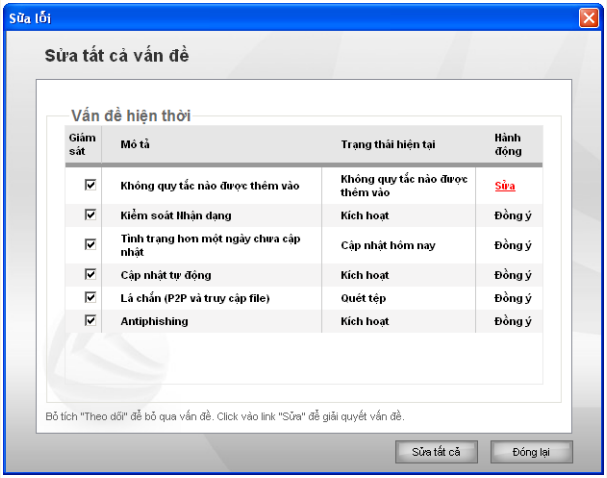
Bốn biểu tượng có thể hiển thị các màu : xanh lục, vàng , đỏ hoặc xám tùy thuộc mức độ bảo vệ.

- **Xanh lục** cho biết máy tính của bạn có ít nguy cơ về an ninh.
- **Vàng** cho biết máy tính của bạn có mức nguy cơ trung bình về an ninh.
- **Đỏ** cho biết máy tính của bạn có nguy cơ về an ninh cao.
- **Grey** một số bộ phận chưa được thiết lập

Sửa mọi vấn đề về bảo mật chỉ bằng một nút kích chuột vào nút **Fix All Issues (Sửa mọi vấn đề)**

Bạn sẽ xem một danh sách tình trạng an ninh và một mô tả ngắn về chúng.

Để sửa lỗi chỉ một vấn đề nhất định thì kích chuột vào nút **Fix (Sửa lỗi)** tương ứng. Nó sẽ giải quyết ngay tại chỗ hoặc sau khi bạn theo một số thao tác được chỉ dẫn. Nếu bạn quyết định sửa lỗi chúng toàn bộ, kích chuột vào nút **Fix All Now (Sửa toàn bộ)** và làm theo hướng dẫn của trình đơn tương ứng.



Vấn đề an ninh

Để khắc phục các vấn đề sau, bấm **Close**.

Quan trọng

Với mỗi vấn đề, có một hộp đánh dấu được kích hoạt mặc định. Nếu bạn không muốn một vấn đề đặc biệt bị đưa vào trong tài khoản khi tính toán các lỗi bảo mật, hãy bỏ lựa chọn trong hộp đánh dấu. Hãy sử dụng tùy chọn này với một chú ý là việc làm trên rất dễ làm tăng khả năng xảy ra các lỗi bảo mật nguy hiểm trong máy tính của bạn.

3.1. Nút tình trạng Virus

Nếu nút tình trạng Virus là xanh lục, thì không có gì phải bận tâm. Tuy nhiên, nếu nút tình trạng Virus là vàng, đỏ hoặc xám, thì nguy cơ về an ninh của máy tính là trung bình hoặc cao.

Màu sắc của nút trạng thái có thể chỉ thay đổi không chỉ khi khi bạn tinh chỉnh các thiết lập có thể ảnh hưởng đến mức độ bảo mật máy tính của bạn, mà còn khi bạn quên không thực hiện công việc quan trọng. Ví dụ, nếu lần quét trước của bạn là đã cũ, nút trạng thái sẽ có màu vàng. Nếu nó đã quá cũ thì nút sẽ chuyển sang màu đỏ.

Bảng dưới đây cung cấp cho bạn thông tin về các yếu tố được đưa vào trong tài khoản khi tính toán mức độ nguy hiểm đến vấn đề bảo mật.

Vấn đề	Màu sắc
Lần quét hệ thống là cũ	Vàng
Lần quét hệ thống là rất cũ	Đỏ
Bảo vệ thời gian thực bị tắt	Đỏ
Mức độ chống virus được đưa về chế độ không bắt buộc	Vàng

Để sửa các vấn đề, làm theo những bước sau:

1. Kích chuột vào nút trạng thái antivirus
2. Sử dụng nút **Giải quyết** để để sửa từng lỗi một hoặc nút **Giải quyết tất** để sử tất cả các lỗi ngay.
3. Nếu như một vấn đề không được sửa ngay lập tức, hãy làm theo wizard để sửa lỗi nó.

3.2. Nút trạng thái Chống Lừa đảo

Nếu như biểu tượng trạng thái của antiphising (chống lừa đảo) ở màu xanh lá cây thì không có gì để lo lắng. Ngược lại, nếu như biểu tượng màu đỏ thì máy bạn có nguy cơ về lỗ hổng bảo mật.

Bảng dưới đây cung cấp cho bạn thông tin về các yếu tố được đưa vào trong tài khoản khi tính toán mức độ nguy hiểm đến vấn đề bảo mật.

Vấn đề	Màu sắc
Chống lừa đảo (antiphising) đang được bật	Xanh lục
Tính năng bảo vệ trước lừa đảo trực tuyến đã bị vô hiệu hóa	Đỏ

Để sửa các vấn đề, làm theo những bước sau:

1. Kích chuột vào nút antiphising.
2. Sử dụng nút **Giải quyết** để để sửa từng lỗi một hoặc nút **Giải quyết tất** để sử tất cả các lỗi ngay.
3. Nếu như một vấn đề không được sửa ngay lập tức, hãy làm theo wizard để sửa lỗi nó.

3.3. Nút Kiểm soát TT Cá nhân

Nếu như nút tình trạng thông tin cá nhân màu lục thì bạn không có gì phải lo lắng. Ngược lại, nếu như nút đó có màu đỏ hay xám, thì có thể máy tính của bạn mắc phải một lỗ hổng bảo mật.

Bảng dưới đây cung cấp cho bạn thông tin về các yếu tố được đưa vào trong tài khoản khi tính toán mức độ nguy hiểm đến vấn đề bảo mật.

Vấn đề	Màu sắc
Tính năng bảo mật được kích hoạt và BẬT	Xanh lục
Tính năng bảo vệ được kích hoạt và TẮT	Đỏ
Tính năng bảo vệ không được kích hoạt	Xám

Để sửa các vấn đề, làm theo những bước sau:

1. Click vào nút trạng thái Kiểm soát Thông tin cá nhân.
2. Sử dụng nút **Giải quyết** để để sửa từng lỗi một hoặc nút **Giải quyết tất** để sử tất cả các lỗi ngay.
3. Nếu như một vấn đề không được sửa ngay lập tức, hãy làm theo wizard để sửa lỗi nó.

3.4. Nút trạng thái nâng cấp

Nếu như biểu tượng update (cập nhập) của bạn màu xanh, không có gì để lo lắng. Ngược lại nếu như biểu tượng màu đỏ thì máy bạn có nguy cơ bị gặp những hiểm họa về bảo mật.

Bảng dưới đây cung cấp cho bạn thông tin về các yếu tố được đưa vào trong tài khoản khi tính toán mức độ nguy hiểm đến vấn đề bảo mật.

Vấn đề	Màu sắc
Nâng cấp tự động được kích hoạt	Xanh lục
Nâng cấp tự động bị vô hiệu hóa	Đỏ
Lần cuối cùng cập nhập đã từ rất lâu rồi	Đỏ

Để sửa các vấn đề, làm theo những bước sau:

1. Kích chuột vào nút update (cập nhập)
2. Sử dụng nút **Giải quyết** để để sửa từng lỗi một hoặc nút **Giải quyết tất** để sử tất cả các lỗi ngay.
3. Nếu như một vấn đề không được sửa ngay lập tức, hãy làm theo wizard để sửa lỗi nó.

4. Các nhiệm vụ nhanh

Phía dưới bốn nút trạng thái có vùng **Nhiệm vụ nhanh**.

4.1. Bảo mật

BitDefender đi với một thành phần bảo mật giúp cho hệ thống của bạn luôn được cập nhập và không có virus

Để vào chức năng Bảo mật, ấn vào thẻ **Bảo mật**.

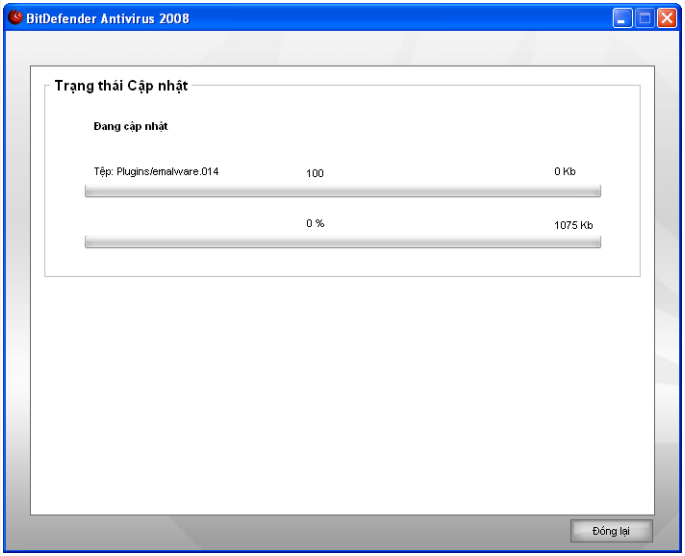
Các nút sau có thể được sử dụng:

- **Cập nhật ngay** - để tiến hành cập nhật ngay.
- **Quét My Document** - khởi động một quá trình quét các văn bản và thiết lập của bạn.
- **Quét sâu hệ thống** - khởi động quá trình quét sâu toàn hệ thống trong máy tính của bạn (kể cả file nén).
- **Quét toàn bộ hệ thống** - khởi động quá trình quét toàn bộ hệ thống trong máy tính của bạn (không kể file nén).

4.1.1. Cập nhật BitDefender

Các chương trình nguy hiểm mới được phát hiện và xác định hàng ngày. Đây là lý do tại sao phải luôn cập nhật BitDefender với các chữ ký mới nhất của các chương trình nguy hiêm.

Theo mặc định, BitDefender tự kiểm tra cập nhật khi bạn bật máy và **từng giờ** sau đó. Nếu bạn cập nhật BitDefender, hãy bấm nút **Cập nhật ngay**. Quá trình cập nhật sẽ bắt đầu và những cửa sổ sau sẽ xuất hiện ngay lập tức:



Cập nhật BitDefender

Bạn không thể thấy được tình trạng trong cửa sổ này.

Quá trình cập nhật đang được thực hiện, có nghĩa là các tệp tin cần cập nhật được thay thế từng bước một. Bằng cách này, quá trình cập nhật sẽ không ảnh hưởng đến hoạt động của sản phẩm mà cũng không bị sơ hở.

Nếu bạn muốn đóng cửa dỗ này, hãy bấm nút **Đóng**. Dù sao, việc này cũng không dừng cập nhật.

Ghi chú
Nếu bạn kết nối với Internet bằng dial-up, bạn nên cập nhật thường xuyên BitDefender theo yêu cầu.

Khởi động lại máy tính. Trong trường hợp cập nhật lớn, bạn có thể được hỏi nếu muốn khởi động lại máy tính.

Nếu bạn không muốn phải bị nhắc lại khi cập nhật đòi hỏi khởi động lại máy, hãy chọn **Chờ khi khởi động, không phải hỏi nữa** Như vậy, lần sau nếu như cập nhật đòi

hỏi phải khởi động máy thì hệ thống vẫn làm việc tiếp cho đến khi bạn muốn tắt hoặc khởi động lại.

Nhấn **Khởi động lại** để khởi đôn ngay lại máy.

Nếu bạn muốn khởi động lại sau, hãy bấm nút **OK**. Chúng tôi khuyên nên khởi động lại càng sớm càng tốt.

4.1.2. Quét bằng BitDefender

Để quét máy tính, chạy từng nhiệm vụ quét một và nhấn vào từng nút tương ứng. Những bảng sau chỉ ra những nhiệm vụ quét, cùng với những chỉ dẫn:

Nh.vụ	*Miêu tả*
Quét My documents	Sử dụng việc quét những thư mục quan trọng: `My Documents`, `Desktop` and `StartUp`. Sẽ bảo đảm hơn cho sự an toàn tài liệu của bạn, một sự an toàn cho công việc và dọn dẹp những ứng dụng chạy lúc máy tính khởi động.
Quét sâu hệ thống	Quét hệ thống này. Ở Cấu hình mặc định, nó sẽ quét tất cả những loại malware đe dọa đến an ninh của hệ thống, cũng như là viruses, spyware, adware, rootkits và những thứ khác.
Quét toàn bộ hệ thống	Quét hệ thống này, trừ tệp tin nén. Ở Cấu hình mặc định, nó sẽ quét tất cả những loại malware đe dọa đến an ninh của hệ thống, cũng như là viruses, spyware, adware, rootkits và những thứ khác.

Ghi chú

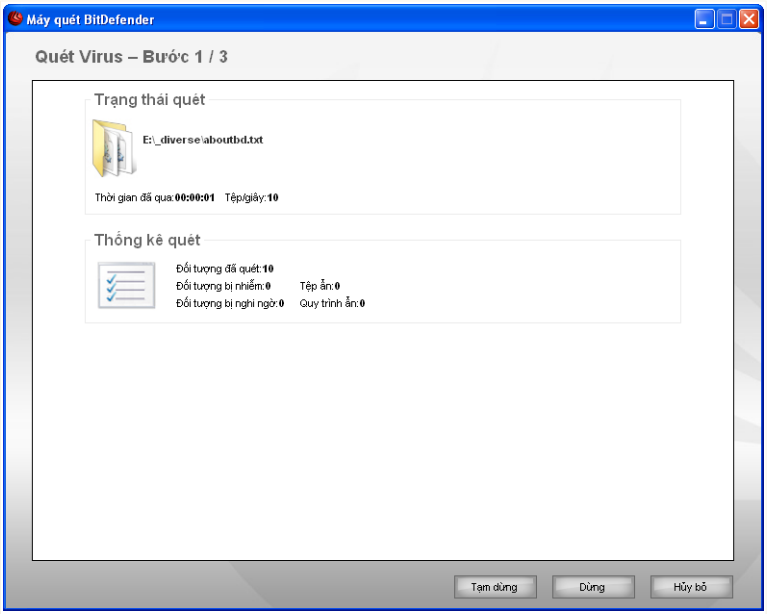
Từ lúc **Quét sâu hệ thống** và **Quét toàn bộ hệ thống** chương trình sẽ tiến hành phân tích toàn bộ hệ thống, tiến trình này có sẽ mất thời gian. Vì vậy chúng tôi khuyên bạn hãy chạy công việc này với mức độ ưu tiên thấp hoặc thấp hơn khi hệ thống của bạn rảnh rỗi

Khi bạn đã quen với quá trình quét "theo mệnh lệnh", thì dù là quét theo chế độ nhanh chóng hay đầy đủ thì BitDefender Scanner cũng sẽ xuất hiện

Làm theo qui trình 3 bước có hướng dẫn để hoàn thành quá trình quét

Bước 1/3 - Đang quét

BitDefender sẽ bắt đầu quét những đối tượng được chọn



Đang quét

Bạn có thể xem thấy tình trạng quét và các thống kê (tốc độ quét, thời gian đã quét, số các đối tượng được quét/bị nhiễm/nghi ngờ...).

Ghi chú

Quá trình quét có thể mất một lhoảng thời gian, tuỳ thuộc vào độ phức tạp của lần quét.

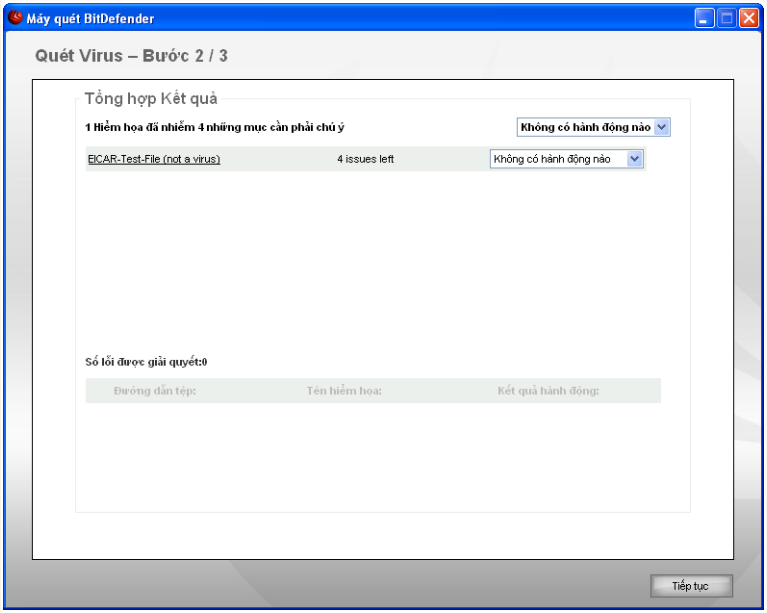
Để tạm thời ngừng quá trình quét, chỉ việc ấn **Tạm dừng**. Bạn sẽ phải ấn **Khôi phục** để khôi phục lại quá trình quét.

Bạn có thể ngừng quá trình quét bất cứ khi nào bạn muốn bằng cách ấn **&Dừng**. Bạn sẽ chuyển đến bước cuối cùng của quá trình trợ giúp (wizard).

Chờ cho BitDenfender hoàn tất quá trình quét.

Bước 2/3 - Chọn cách thực hiện

Khi quá trình quét đã hoàn thành, một cửa sổ mới sẽ xuất hiện, nơi bạn có thể xem kết quả quét.



Hành động

Bạn có thể xem một số ảnh hưởng đến máy tính của bạn.

Những đối tượng bị nhiễm hiển thị theo nhóm, trên cơ sở malware gây nhiễm. Click link tương ứng với hiểm họa để tìm thông tin về những đối tượng bị nhiễm.

Bạn có thể chọn một hành động toàn diện cho mỗi nhóm vấn đề hoặc bạn cũng có thể tách riêng từng hành động cho mỗi vấn đề.

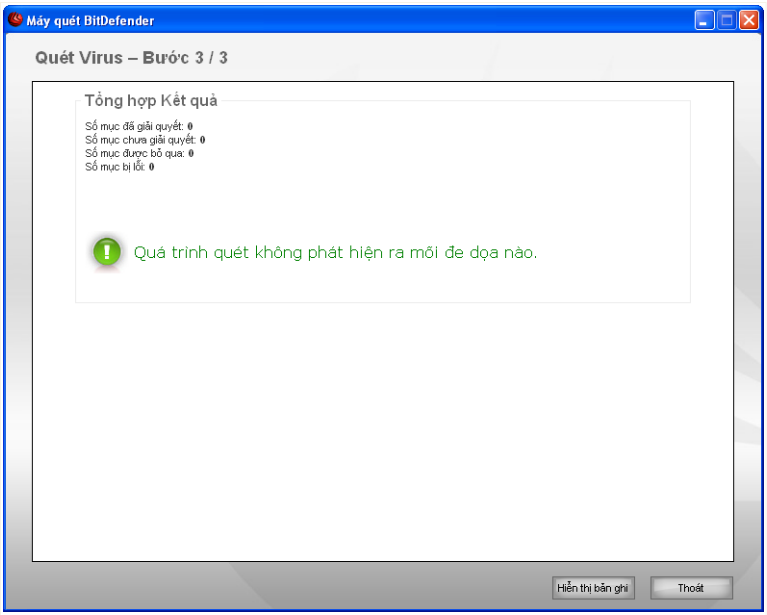
Các tùy chọn trên có thể xuất hiện ở trình đơn:

Hành động	Miêu tả
Không thực thi	Không có hành động nào được tiến hành đối với các tập tin đã nhận diện.
Loại bỏ mã độc	Làm sạch tập tin bị nhiễm.
Xoá	Xóa những tệp tin đã nhận diện.
Bỏ ẩn	Làm hiện các đối tượng đang ẩn.

Nhấn **Tiếp** để áp dụng hành động đã định.

Bước 3/3 - Xem kết quả

Khi BitDenferder kết thúc quá trình sửa vấn đề, kết quả quét sẽ xuất hiện ở một cửa sổ mới



Tổng kết

Bạn có thể xem bảng tổng hợp kết quả.

Nếu như những tệp tin bị nghi ngờ được tìm thấy trong quá trình quét, bạn sẽ được yêu cầu gửi chúng đến BitDefender Lab. File nghi vấn được phát hiện bởi phân tích hành vi và chúng có thể nhiễm với chữ ký mã độc mới mà chưa được biết tới.

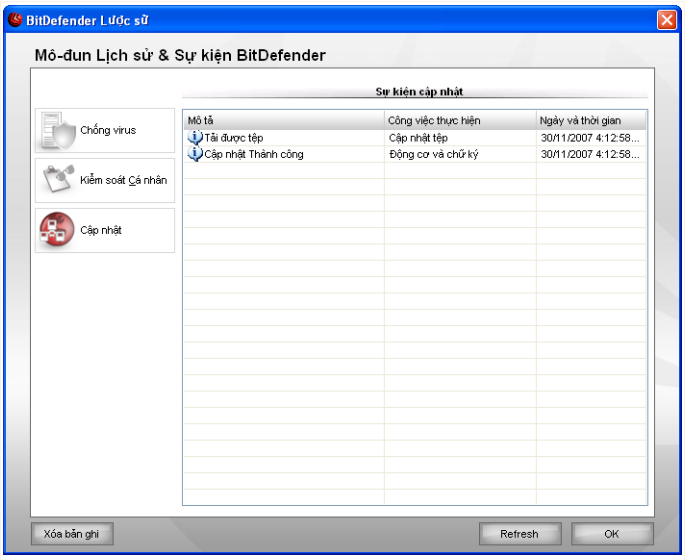
Tập tin báo cáo sẽ tự động được lưu trong phần Nhật kí hệ thống từ cửa sổ **Thuộc tính** của nhiệm vụ tương ứng.

Cảnh báo

Nếu như có những vấn đề chưa giải quyết được, chúng tôi khuyến cáo bạn nên liên lạc với BitDefender Support Team tại www.bitdefender.com.

5. Lịch sử

Liên kết **Lịch sử** ở cuối cửa sổ BitDefender Security Center sẽ mở ra một cửa sổ khác hiển thị lịch sử các sự kiện của BitDefender &. Cửa sổ này sẽ cung cấp cho bạn một cái nhìn tổng quát về các sự kiện bảo mật liên quan. Ví dụ, bạn sẽ dễ dạng kiểm tra nếu việc nâng cấp thành công, Nếu malware được tìm thấy trong máy tính của bạn, nếu việc sao lưu không gặp lỗi,...v.v.



Các sự kiện

Để giúp bạn lọc các thông tin về lịch sử hoạt động của BitDefender &, Các nhóm kèm theo được cung cấp ở vùng bên trái:

- **Antivirus**
- **Điều khiển cá nhân**
- **Cập nhật**

Một danh sách các sự kiện có hiệu lực cho mỗi nhóm. Mỗi sự kiện được kèm theo các thông tin: mô tả ngắn gọn, cách BitDefender thực hiện khi sự kiện xảy ra, và ngày

tháng thời gian nó xảy ra. Nếu bạn muốn tìm thêm thông tin về một sự kiện cụ thể trong danh sách, hãy ấn đúp chuột vào sự kiện đó.

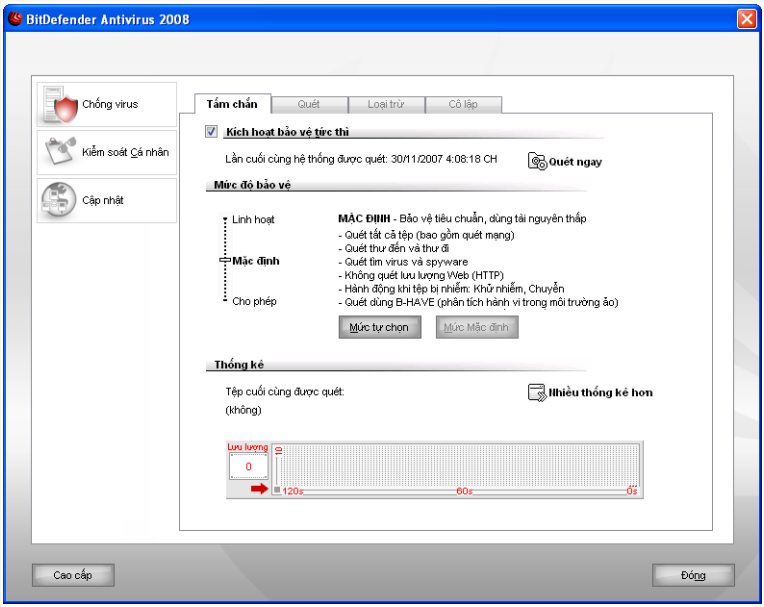
Ấn vào **Xóa sạch nhật kí hệ thống** nếu bạn muốn gỡ bỏ nhật kí hệ thống cũ hoặc nhấp vào **Làm tươi** để chắc chắn nhật kí mới nhất được hiển thị.

Quản lý an ninh cấp cao

6. Bắt đầu

BitDefender Antivirus 2008 có một bảng điều khiển thiết lập trung tâm, cho phép các cấu hình nâng cao và hệ quản trị của BitDefender.

Để truy xuất vào bảng điều khiển thiết lập, Ấn vào liên kết **Thiết lập** , ở phía dưới của cửa sổ Security Center.



Bảng điều khiển thiết lập

Bảng điều khiển thiết lập được sắp xếp theo các chức năng: **Antivirus**, **Điều khiển cá nhân** và **Cập nhật**. Cho phép bạn dễ dàng quản lý BitDefender dựa trên kiểu địa chỉ bảo mật.

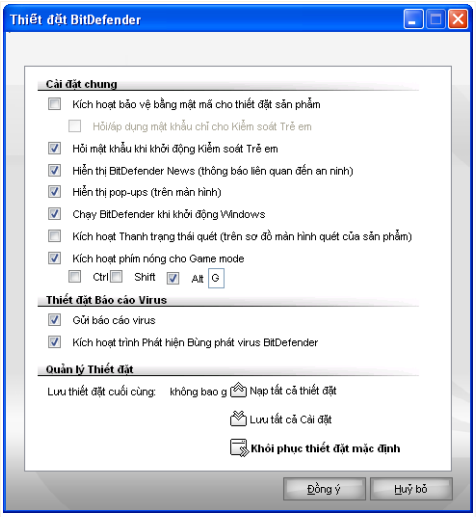
Ở phía trái bảng điều khiển thiết lập, bạn có thể nhìn thấy chức năng chọn lọc:

- Antivirus - Trong phần này, bạn có thể mặc định module **Antivirus**.

- Kiểm soat Riêng tư - bạn có thể thiết lập thông số cho chức năng**Kiểm soat Riêng tư**.
- Update - Trong phần này, bạn có thể mặc định module **Update**.

6.1. Cấu hình các thiết lập chung

Để cấu hình các thiết lập chung cho BitDefender Antivirus 2008 và quản lý các thiết lập của nó, ấn **Nâng cao**. Một cửa sổ mới sẽ được hiện ra



Các phần cài đặt chung

Tại dây, bạn có thể thiết lập hành vi tổng quát của BitDefender. Bằng mặc định, BitDefender được tải tại phần khởi động Windows và sau đó vận hành tối thiểu tại thanh tác vụ.

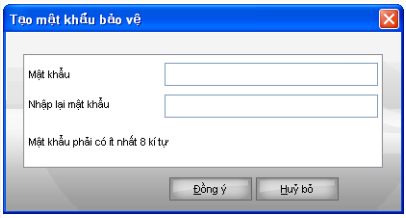
6.1.1. Các phần cài đặt chung

- **Kích hoạt bảo vệ mật khẩu cho cấu hình sản phẩm** - Cho phép thiết lập một mật khẩu để bảo vệ cấu hình Bảng của BitDefender.

Ghi chú

Nếu bạn không phải là người duy nhất có quyền sử dụng máy tính này thì chúng tôi khuyên bạn nên bảo về các phần cài đặt BitDefender của mình bằng một mật khẩu.

Nếu bạn chọn phương án này thì cửa sổ tiếp theo sẽ xuất hiện:



Vào mật khẩu

Đánh mật khẩu vào trường **Mật khẩu**, đánh lại vào trường **Gõ lại mật khẩu** và nhấp chuột vào **OK**.

Khi bạn có mật khẩu, bạn sẽ được hỏi bạn muốn giữ thay đổi cấu hình của BitDefender cho đến bao giờ. Người quản trị hệ thống (nếu có) phải cung cấp mật khẩu để thay đổi cấu hình BitDefender.

Quan trọng

Nếu bạn quên mật khẩu, bạ sẽ phải sửa chữa sản phẩm để thay đổi cấu hình của BitDefender.

- **Hiện thị các tin tức của BitDefender (các thông báo liên quan đến an ninh)** - hiển thị liên tục các thông báo an ninh liên quan đến sự bùng phát virus, do máy chủ BitDefender gửi tới.
- **Hiển thi các trình đơn (Các ghi chú trên màn hình on-screen notes)** - Hiển thi các trình đơn về tình trạng sản phẩm.
- **Tải BitDefender tại phần khởi động của Windows** - Tự động đưa ra BitDefender khi khởi động hệ thống. Chúng tôi khuyến cáo bạn nên tiếp tục chọn phương án này.
- **Cho phép thanh Hoạt động quét (trên đồ thị màn hình của hoạt động sản phẩm)** - được phép/ không được phép Thanh hoạt đọng Quét .
- **Kích hoạt phím nóng Chế độ Game** - cho phép dùng tổ hợp các phím nóng (hotkey) để kích hoạt / ngừng Chế độ Game. Phín nóng (hotkey) mặc định là `Alt+G`.

  Để thay đổi phím nóng, làm như sau:

  1. Kiểm tra sự thay đổi phím mà bạn muốn dùng như sau: phím Control (`Ctrl`), phím Shift (`Shift`) hoặc phím Alternate (`Alt`).
  2. Trong trường sửa, gõ chữ tương ứng với phím mà bạn muốn dùng.

6.1.2. Cài đặt Báo cáo về Virus

- **Gửi báo cáo về virus** - gửi tới các phòng thí nghiệm của BitDefender Labs các báo cáo về virus được xác định trong máy tính của bạn. Chúng giúp chúng tôi theo được dấu vết những đợt bùng nổ virus.

  Các báo cáo sẽ không chứa đựng những thông tin bí mật như tên của bạn, địa chỉ IP và các thông tin khác và sẽ không được sử dụng cho các mục đích thương mại. Thông tin được cung cấp sẽ chỉ chứa tên của virus và sẽ được sử dụng với mục đích duy nhất là thiết lập các báo cáo mang tính chiến lược.
- **Cho phép BitDefender phát hiện Sự bùng nổ Virus của BitDefender Outbreak Detection** - Gửi đến các phòng thí nghiệm của BitDefender các báo cáo về những đợt bùng nổ virus có khả năng xảy ra.

  Các báo cáo sẽ không chứa đựng những thông tin bí mật như tên của bạn, địa chỉ IP và các thông tin khác và sẽ không được sử dụng cho các mục đích thương mại. Thông tin được cung cấp sẽ chỉ chứa tên virus tiềm tàng và sẽ được sử dụng với mục đích duy nhất là phát hiện các virus mới.

6.1.3. Quản lý cài đặt

Sử dụng **Lưu tất cả các phần cài đặt** / **Tải tất cả các phần cài đặt** các nút để lưu / Tải các phần bạn vừa cài đặt cho BitDefender vào vị trí theo ý muốn. Bằng cách này, bạn có thể sử dụng lại các phần cài đặt này khi bạn cài đặt lại hoặc sửa chữa sản phẩm BitDefender.

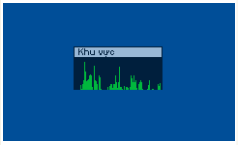
Quan trọng
Chỉ những người sử dụng có quyền quản lý mới có thể lưu và tải các phàn cài đặt.

Để nạp thiết lập mặc định **Khôi phục thiết lập mặc định**.

6.2. Sử dụng Scan Activity Bar

Thanh hoạt động quét là một biểu tượng trực quan của hoạt động quét trong hệ thống của bạn.

Các thanh màu xanh (**File Zone**) hiển thị số các tập tin được quét mỗi giây, theo tỉ lệ từ 0 to 50.



Thanh Hoạt động

Ghi chú

Thanh trạng thái hoạt động Quét sẽ lưu ý bạn khi việc bảo vệ thời gian thực(real-time protection) bị tắt bằng cách hiển thị một đường thẳng đỏ đi qua **File Zone**.

Bạn có thể sử dụng **Scan activity bar** để quét các đối tượng. Chỉ việc kéo các đối tượng bạn muốn quét và thả chúng vào đó.

Ghi chú

Để có thêm thông tin , hãy chuyển đến "*Quét kéo và thả*" (p. 63).

Khi bạn không muốn xem biểu tượng trực quan nữa, bạn chỉ cần nhấp chuột phải vào đó và chọn **Ẩn** . Để ẩn hoàn toàn cửa sổ này, Ấn vào **Nâng cao** trong bảng điều khiển thiết lập và bỏ lựa chọn tại hộp kiểm tra tương ứng để **Kích hoạt thanh trạng thái hoạt động Quét (trên màn hình đồ thị về hoạt động của sản phẩm)**.

7. Antivirus

BitDefender bảo vệ máy tính của bạn khỏi tất cả các loại malware (virus, Trojan, spyware, rootkit...)

Bên cạnh việc quét bằng phương pháp truyền thống dựa trên các malware đã biết. BitDefender còn thực hiện phân tích heuristic khi quét các tệp tin. Mục tiêu của việc quét bằng phương pháp heuristic là để xác định những virus mới, dựa trên các kiểu, dạng, các thuật toán nhất định, trước khi biết rõ về loại virus đó. Các thông điệp cảnh sẽ xuất hiện khi một tập tin như vậy được phát hiện và được liệt vào loại bị nghi ngờ. Trong những trường hợp đó, chúng tôi khuyến cáo bạn nên gửi tới phòng thí nghiệm của BitDefender để được phân tích.

Các phần bảo vệ do BitDefender cung cấp được chia ra thành hai loại:

- **Quét khi sử dụng** - ngăng ngừa các malware mới xâm nhập vào hệ thống của bạn. Đây cũng còn được gọi là bảo vệ thời gian thực - các tệp tin được quét kiểm tra ngay khi bạn sử dụng chúng. Ví dụ BitDefender sẽ quét một từ của tài liệu bị nghi ngờ khi bạn mở nó, và một e-mail khi bạn nhận nó.
- **Quét theo yêu cầu** - cho phép phát hiện và xóa malware thường trú từ trước trong hệ thống của bạn. Đây là kiểu quét truyền thống do người sử dụng khởi xướng - bạn chọn ổ đĩa, thư mục hoặc tập tin nào mà BitDefender phải quét và BitDefender quét chúng theo yêu cầu. Việc quét cho phép bạn tùy biến cá nhân quá trình quét và chúng có thể lên lịch để chạy trong một cơ sở thường nhật

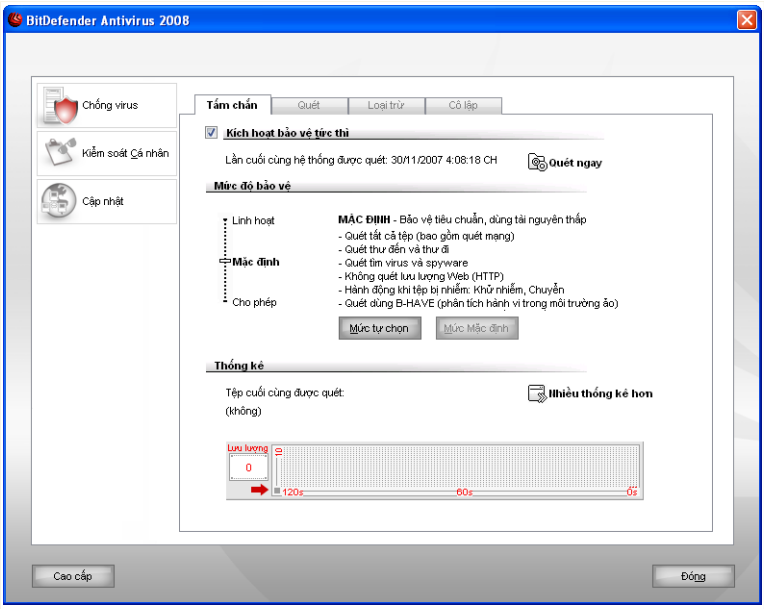
Phần **Chốngvirus** của hướng dẫn sử dụng này chứa đựng các đề tài sau:

- Quét khi truy cập
- Quét theo yêu cầu
- Các đối tượng được bỏ qua khi quét
- Vùng cách ly

7.1. Quét khi truy cập

Quét khi thực thi, còn được gọi là bảo vệ thời gian thực, giữ cho máy tính của bạn an toàn khỏi tất cả các loại malware bằng cách quét các tập tin được truy cập, các tin nhắn e-mail và các giao tiếp qua các ứng dụng phần mềm truyền tin nhanh (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Để cấu hình và theo dõi việc bảo vệ thời gian thực, ấn vào **Antivirus>Shield** trong bảng điều khiển thiết lập. Cửa sổ kế tiếp hiện ra:



Bảo vệ đúng lúc

Quan trọng
Để ngăn chặn virus xâm nhập vào máy tính của bạn, hãy giữ khả năng hoạt động cho cho **bảo vệ đúng lúc** .

Tại cacnhj đáy của phần này, bạn có thể nhìn thấy các số liệu thống kê **Bảo vệ đúng lúc** về các tập tin và các thư điện tử đã được quét. Nhấp vào **Thêm số liệu thống kê** nếu như bạn muốn xem một cửa sổ giải thích chi tiết hơn về các số liệu thống kê này.

Để bắt đầu quét nhanh hệ thống, ấn **Quét ngay**.

7.1.1. Cấu hình cấp độ bảo vệ

Bạn có thể chọn mức bảo vệ phù hợp hơn với các yêu cầu an ninh của bạn. Hãy kéo thanh trượt dọc theo mặt chia độ để chọn mức bảo vệ phù hợp.

Có 3 mức bảo vệ:

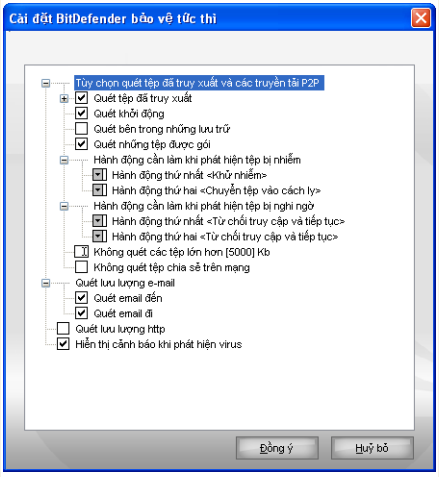
Mức bảo vệ	Miêu tả
Được chấp nhận	Bao quát các yêu cầu an ninh cơ bản. Mức tiêu thụ tài nguyên rất thấp. Các chương trình và các thông điệp thư điện tử chỉ được quét virus. Ngoài việc quét dựa trên chữ ký cổ điển, việc phân tích để phát hiện cũng được sử dụng. các hành động được tiến hành đối với các tập tin bị nhiễm như sau: làm sạch tập tin/ từ chối truy cập.
Mặc định	Giữ mức an ninh tiêu chuẩn. Mức tiêu thụ tài nguyên thấp. Tất cả các tập tin và các thư điện tử đến và đi đwocj quét virus và các chương trình gián điệp. Ngoài việc quét dựa trên chữ ký cổ điển, việc phân tích để phát hiện cũng được sử dụng. các hành động được tiến hành đối với các tập tin bị nhiễm như sau: làm sạch tập tin/ từ chối truy cập.
Tấn công	Giữ an ninh ở mức cao. Mức tiêu thụ tài nguyên trung bình. Tất cả các tập tin, các thư điện tử đến và đi cũng như lưu lượng thông tin web được quét virus và các chương trình gián điệp. Ngoài việc quét dựa trên chữ ký cổ điển, việc phân tích để phát hiện cũng được sử dụng. các hành động được tiến hành đối với các tập tin bị nhiễm như sau: làm sạch tập tin/ từ chối truy cập.

Để áp dụng thiết lập bảo vệ thời gian thực mặc định ấn **Mức Mặc định** .

7.1.2. Tuỳ biến cấp độ bảo vệ

Những người dùng có trình độ cao có thể muốn tận dụng các lợi thế của các thiết lập quét do BitDefender cung cấp. Công cụ quét có thể được thiết lập chỉ để quét các phần mở rộng riêng, để tìm một loại malware đặc biệt hay bỏ qua tập tin nén. Việc này giảm đi đáng kể thời gian quét và cải thiện sự thích ứng của máy tính trong một lần quét.

Bạn có thể tuỳ chỉnh **Real-time protection**bằng cách nhấp **Custom level**. Cửa sổ sau đây sẽ xuất hiện:



Cài đặt Lá chắn

Các phương án quét được tổ chức giống như một thực đơn có thể mở rộng, rất giống với các phương pháp duyệt (exploring) của Windows. Nhấp vào hộp có "+" để mở một phương án hoặc vào hộp có "-" để đóng một phương án.

Ghi chú

Bạn có thể quan sát thấy là một số phương án quét không thể mở ra được mặc dù dấu "+" đã xuất hiện. Lý do là các phương án này còn chưa được lựa chọn. Bạn sẽ thấy nếu bạn chọn chúng, chúng sẽ có thể mở ra được.

- **Quét các tập tin đã được truy cập và các phương án chuyển P2P** - quét các tập tin được truy cập và các giao tiếp qua các ứng dụng phần mềm truyền tin nhanh (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Tiếp theo, chọn lợi các tập tin mà bạn muốn quét.

Phương án		*Miêu tả*
Quét file kích hoạt	**Quét tất cả các tập tin**	Tất cả các tập tin đã được truy cập sẽ được quét, bất kể chúng thuộc loại nào.
	Chỉ quét các tập tin chương trình	Chỉ có các tập tin chương trình sẽ được quét. điều này có nghĩa là các tập tin với những

Phương án		Miêu tả
		phần mở rộng sau:.exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws.
	Quét các phần mở rộng do người sử dụng xác định	Chỉ các tập tin với những phần mở rộng do người sử dụng chỉ ra sẽ được quét. Những phần mở rộng này phải được tách ra bằng ";".
	Quét cho phần có nguy cơ	Quét bộ nhớ để tìm các chương trình vụng trộm. Những tập tin bị nhận dạng sẽ được coi là những tập tin bị nhiễm. Phần mềm bao gồm các thành phần quảng cáo có thể bị ngừng hoạt động nếu như tùy chọn này được kích hoạt. Chọn **Bỏ qua, không quét dialers và các ứng dụng** nếu bạn muốn bỏ qua, không quét các tập tin thuôvj loại này.
Quét khởi động		Quét các rãnh ghi của hệ thống.
Quét các tệp lưu trữ bên trong		Các tệp lưu trữ được truy xuất sẽ được quét. Với phương án này, máy tính của bạn sẽ chạy chậm lại.
Quét các tập tin được đóng gói		All packed files will be scanned.
Hành động đầu tiên		Chọn từ thực đơn rơi bên dưới hành động đầu tiên để lấy ra các tập tin bị nhiễm hoặc bị nghi ngờ.
	Từ chối truy cập và tiếp tục	Trong trường hợp một tập tin bị nhiễm được phát hiện, việc truy cập tập tin đó sẽ bị từ chối.
	làm sạch tập tin	Làm sạch tập tin bị nhiễm.
	Xoá tập tin	Xoá các tập tin bị nhiễm ngay lập tức, không cần cảnh báo.

Phương án		Miêu tả
	Chuyển đến nơi kiểm dịch	Chuyển các tập tin bị nhiễm đến Vùng cách ly.
Hành động thứ hai		Chọn từ thực đơn rơi bên dưới hành động thứ hai để để xử lý tập tin bị nhiễm nếu như hành động thứ nhất thất bại.
	Từ chối truy cập và tiếp tục	Trong trường hợp một tập tin bị nhiễm được phát hiện, việc truy cập tập tin đó sẽ bị từ chối.
	Xoá tập tin	Xoá các tập tin bị nhiễm ngay lập tức, không cần cảnh báo.
	Chuyển đến nơi kiểm dịch	Chuyển các tập tin bị nhiễm đến Vùng cách ly.
Đừng quét các tập tin có dung lượng lớn hơn [x] Kb		Hãy đánh vào kích thước lớn nhất của các tập tin chuẩn bị quét. Nếu dung lượng của tập tin là 0 Kb, tất cả các tập tin sxẽ được quét, bất kể kích thước như thế nào.
Không quét các chia sẻ mạng		Nếu tùy chọn này đã được kích hoạt, BitDefender sẽ không quét các chia sẻ mạng, cho phép chúng truy cập được nhanh hơn. Chúng tôi khuyến cáo bạn chỉ nên kích hoạt tùy chọn này nếu một phần hệ thống mạng đã được bảo vệ bởi một trình diệt virus.

- **Quét lưu lượng thư điện tử** - Quét lưu lượng thư điện tử.

  Có những lựa chọn sau:

Phương án	Miêu tả
Quét các thư đến	Quét tất cả các thư đến.
Quét các thư đi	Quét tất cả các thư đi.

- **Quét lưu lượng http** - Quét lưu lượng http.
- **Hiển thị cảnh báo virus đã được tìm ra** - Mở một cửa sổ cảnh báo khi virus được tìm thấy ở một tập tin hoặc ở trong một thư điện tử.

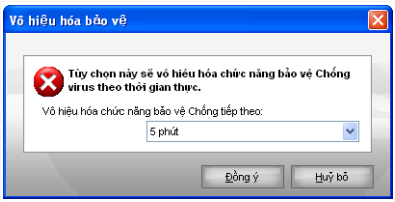
Đối với một tập tin bị nhiễm, cửa sổ cảnh báo sẽ chứa tên của virus,đường dẫn đến virus đó và hành động của BitDefender và đường kết nối với vị trí của BitDefender, nơi bạn có thể tìm thấy thêm thông tin về nó. Đối với một thư điện tử bị nhiễm, cửa sổ cảnh báo cũng sẽ chứa các thông tin về người gửi và người nhận.

Trong trường hợp một tập tin bị nghi ngờ được phát hiện, bạn có thể khởi động wizard từ cửa sổ cảnh báo, nó sẽ giúp bạn gửi tập tin đó đến phòng thí nghiệm của BitDefender Lab để phân tích sâu hơn. Bạn có thể đánh địa chỉ thư điện tử của bạn đẻ nhận các thông tin liên quan đến báo cáo này.

Nhấp **OK**để lưu lại các thay đổi và đóng cửa sổ lại.

7.1.3. Tắt Bảo vệ thời gian thực

Nếu bạn muốn tắt chế độ bảo vệ thời gian thực, một cửa sổ cảnh báo sẽ xuất hiện:



Tắt Bảo vệ thời gian thực

Bạn phải xác nhận lựa chọn của bạn bằng cách chọn từ menu rằng bạn muốn vô hiệu hóa tạm thời chế độ bảo vệ thời gian thực trong bao lâu. Bạn có thể vô hiệu hóa tạm thời sự bảo vệ trong 5,15 hoặc phút, một giờ, vĩnh viễn hoặc cho đến khi nào hệ thống khởi động lại.

Cảnh báo
Đây là một lỗ hổng bảo mật nguy hiểm. Chúng tôi đề nghị bạn chỉ nên tắt chế độ bảo vệ thời gian thực trong một khoảng thời gian ngắn nhất có thể. Nếu chế độ này bị tắt, bạn sẽ không được bảo vệ khỏi các maiware.

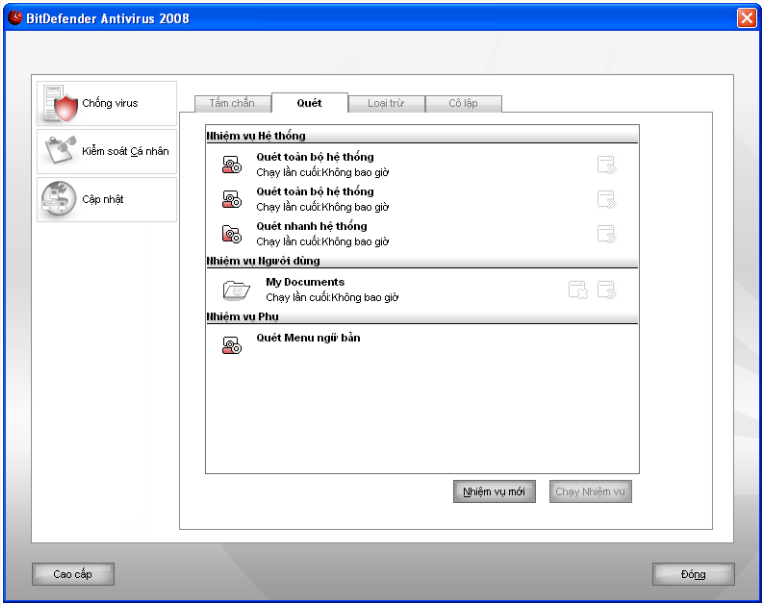
7.2. Quét theo yêu cầu

Mục tiêu chính của BitDefender là giữ cho máy tính của bạn sạch virus. Điều đầu tiên, cần thiết nhất phải làm là giữ không cho các virus mới xâm nhập vào máy tính của

bạn và quét các thư điện tử của bạn, tất cả các tập tin được truy cập hoặc sao chép vào máy tính của bạn.

Có nguy cơ là một virus đã nằm sẵn trong máy tính của bạn, thậm chí là trước khi bạn cài đặt BitDefender. Chính vì thế, sẽ là một ý tưởng hay nêu snhư bạn quét máy tính của mình để loại trừ các virus thường trú sau khi bạn lắp đặt xong BitDefender. và dĩ nhiên, sẽ rất tốt nếu bạn thường xuyên quét máy tính để loại trừ virus.

Để cấu hình và làm quen với chế độ quét theo yêu cầu, ấn vào **Antivirus>Scan** trong bảng điều khiển thiết lập. Cửa sổ kế tiếp hiện ra:



Các nhiệm vụ quét

Quét theo yêu cầu được thiết lập cơ bản trong các nhiệm vụ quét. Nhiệm vụ quét chỉ rõ các tùy chọn quét và các đối tượng được quét. Bạn có thể quét máy tính bất kì khi nào bạn muốn bằng cách chạy công tác mặc định hoặc bạn có thể làm chủ quá trình này. Bạn cũng có thể lên lịch cho chúng chạy theo một qui luật đơn giản hoặc khi hệ thống bạn nhẹ tải và không làm ảnh hưởng đến công việc của bạn.

7.2.1. Các nhiệm vụ quét

BitDefender chạy cùng với một số nhiệm vụ được thiết lập mặc định, chúng có thể quản lý được một số lỗ hổng bảo mật chung nhất. Bạn cũng có thể thiết lập quá trình quét của riêng bạn.

Mỗi một công tác có một cửa sổ **Thuộc tính** cho phép bạn cấu hình công tác đó và xem kết quả quá trình quét. Để có thêm thông tin, hãy chuyển đến "*Cấu hình nhiệm vụ quét*" (p. 51).

Có ba phạm trù của các nhiệm vụ quét:

- **Các nhiệm vụ Hệ thống** - chứa danh sách các nhiệm vụ hệ thống được mặc định. Có những nhiệm vụ sau:

Nhiệm vụ mặc định	*Miêu tả*
Quét sâu hệ thống	Quét hệ thống này. Ở Cấu hình mặc định, nó sẽ quét tất cả những loại malware đe dọa đến an ninh của hệ thống, cũng như là viruses, spyware, adware, rootkits và những thứ khác.
Quét toàn bộ hệ thống	Quét hệ thống này, trừ tệp tin nén. Ở Cấu hình mặc định, nó sẽ quét tất cả những loại malware đe dọa đến an ninh của hệ thống, cũng như là viruses, spyware, adware, rootkits và những thứ khác.
Quét nhanh Hệ thốngQuick System Scan	Quét `Windows`, `Program Files` và thư mục `All Users`. Ở cấu hình mặc định, nó sẽ quét tất cả những loại malware, ngoại trừ rootkits, nhưng nó sẽ không quét bộ nhớ, registry hoặc cookies.

Ghi chú

Từ lúc **Quét sâu hệ thống** và **Quét toàn bộ hệ thống** chương trình sẽ tiến hành phân tích toàn bộ hệ thống, tiến trình này có sẽ mất thời gian. Vì vậy chúng tôi khuyên bạn hãy chạy công việc này với mức độ ưu tiên thấp hoặc thấp hơn khi hệ thống của bạn rảnh rỗi

- **Các nhiệm vụ của người sử dụng** - chứa các nhiệm vụ do người sử dụng xác định.

  Một hành động mở `My Documents` được gọi. Sử dụng những công tác quét những thư mục quan trọng của người sử dụng: `My Documents`, `Desktop` and `StartUp`.

Sẽ bảo đảm hơn cho sự an toàn tài liệu của bạn, một sự an toàn cho công việc và dọn dẹp những ứng dụng chạy lúc máy tính khởi động.

- **Các nhiệm vụ hỗn hợp** - Chứa danh sách các nhiệm vụ quét hỗn hợp. Những nhiệm vụ quét này chỉ những dạng quét thay thế mà không thể vận hành được từ cửa sổ này. You can only modify their settings or view the scan reports.

Có ba nút ở bên phải mỗi một nhiệm vụ:

- **Nhiệm vụ theo lịch** - chỉ ra rằng nhiệm vụ được chọn đã được lên lịch cho thời gian sau này. Nhấp vào nút này để tới phần Scheduler từ các cửa sổ **Properties** nơi bạn có thê sửa đổi phần cài đặt này.
- **Xoá** - Bỏ nhiệm vụ được chọn.

> ***Ghi chú***
> Không có đối các nhiệm vụ hệ thống. Bạn không thể huỷ bỏ một nhiệm vụ hệ thống.

- **Scan Now** - vận hành một nhiệm vụ được chọn, khởi động một immediate scan.

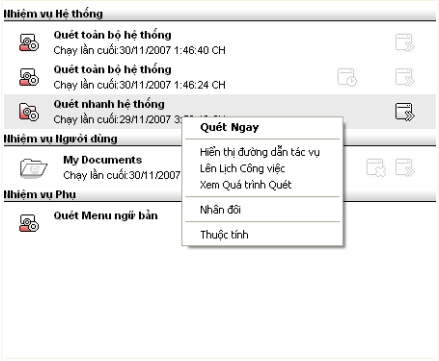
Mỗi nhiệm vụ quét có cửa sổ **Thuộc tính** nơi bạn có thể cấu hình các tùy chọn quét, hãy đặt mục tiêu quét, lập kế hoạch cho nhiệm vụ hoặc xem các báo cáo.

7.2.2. Thực đơn tắt

Mỗi nhiệm vụ có một thực đơn tắt. Nhấp chuột phải vào nhiệm vụ được chọn để mở thực đơn này:

Các liệnh sau đây có sẵn trên thực đơn tắt:

- **Quét bây giờ** - vận hành hoạt động được chọn, khởi xướng một hành động quét ngay lập tức.
- **Đường dẫn** - Mở cửa sổ **Thuộc tính** , thẻ Đường dẫn, tại đây bạn có thể thay đổi mục tiêu quét cho nhiệm vụ được chọn.



Thực đơn tắt

Ghi chú
trong trường hợp nhiệm vụ hệ thống, lựa chọn này được thay bằng **Hiển thị đường dẫn nhiệm vụ**, để bạn có thể thấy được đích quét của chúng.

- **Nhiệm vụ lập kế hoạch** - mở cửa sổ **Thuộc tính**, thẻ Nhiệm vụ lập kế hoạch, tại đây bạn có thể lập kế hoạch cho mộ nhiệm vụ được chọn
- **Nhật kí hệ thống** - Mở cửa sổ **Thuộc tính**, thẻNhật kí hệ thống tại đây, bạn có thể xem các báo cáo phát sinh sau khi niệm vụ được chọn vận hành;
- **Nhân bản** - Nhân bản nhiệm vụ được chọn;

Ghi chú
Phần này có tác dụng khi lập các nhiệm vụ mới bởi vì bạn có thể sửa đổi các nội dung cài đặt liên quan đến nhân bản nhiệm vụ.

- **Xoá** - xoá nhiệm vụ được chọn.

Ghi chú
Không có đối các nhiệm vụ hệ thống. Bạn không thể huỷ bỏ một nhiệm vụ hệ thống.

- **Mở** - mở cửa sổ **Thuộc tính**, thẻ Tổn quát , tại đây bạn có thể thay đổi các phần cài đặt của nhiệm vụ được chọn.

Ghi chú
Do tính chất đặc biệt của chúng, chỉ có các phương án **Properties** và **View Scan Logs** có sẵn cho các nhiệm vụ trong phạm trù **Các nhiệm vụ linh tinh** .

7.2.3. Tạo các nhiệm vụ quét

Để tạo một nhiệm vụ quét, bạn có thể chọn một trong các hành động sau đây:

- Nhân bản một nhiệm vụ hiện hành, đổi tên nhiệm cụ đó và tạo các thay đổi cần thiết trong cửa sổ Thuộc tính .
- Ấn **Nhiệm vụ mới** để tạo ra một nhiệm vụ mới và cấu hình nó.

7.2.4. Cấu hình nhiệm vụ quét

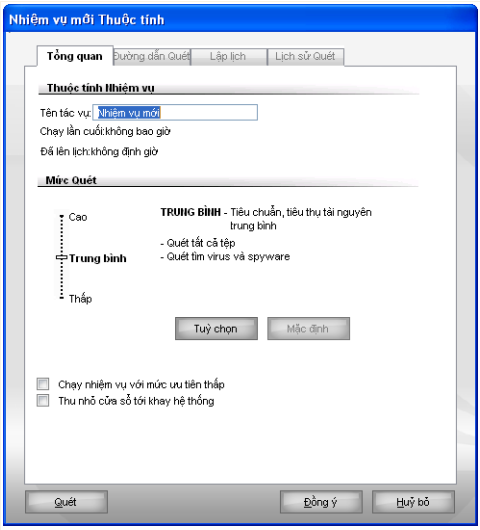
Mỗi nhiệm vụ quét có cửa sổ **Thuộc tính** nơi bạn có thể cấu hình các tùy chọn quét, hãy đặt mục tiêu quét, lập kế hoạch cho nhiệm vụ hoặc xem các báo cáo. Để mở cửa sổ này nhấn nút **Mở**, nằm phía bên phải của nhiệm vụ (hoặc nhấp phải chuột và chọn) **Mở**.

Ghi chú

Để biết thêm chi tiết khi xem nhật kí và thẻ **Nhật kí hệ thống**, hãy chuyển đến "*Xem nhật kí quét*" (p. 68).

Cấu hình thiết lập quét

Để cấu hình tùy chọn quét của một nhiệm vụ cụ thể, nhấp phải chuột và chọn **Tính chất**. Cửa sổ kế tiếp hiện ra:



Tổng quan

Tại đây, bạn có thể xem các thông tin về những nhiệm vụ (tên, lần vận hành cuối cùng, và tình trạng kế hoạch) và tiến hành cài đặt quét.

Chọn cấp độ quét

Bạn có thể dễ dàng cấu hình thiết lập quét bằng cách chọn cấp độ quét. Kéo con trượt dọc theo bảng chia độ để đặt cấp độ quét phù hợp.

Có tất cả 3 cấp độ:

Mức bảo vệ	Miêu tả
Thấp	Cung cấp hiệu suất phát hiện hợp lý. Mức tiêu thụ tài nguyên thấp. Các chương trình chỉ được quét virus. Ngoài việc quét dựa trên chữ ký cổ điển, phép phân tích heuristic cũng được sử dụng.
Trung bình	Cung cấp hiệu suất phát hiiện tốt. Mức tiêu thụ tài nguyên trung bình. Tất cả các tập tin đều được quét virus và các phần mềm gián điệp. Ngoài việc quét dựa trên chữ ký cổ điển, phép phân tích heuristic cũng được sử dụng.
Cao	Cung cấp hiệu suất phát hiiện cao. Mức tiêu thụ tài nguyên cao. Tất cả các tập tin và các tài liệu lưu trữ đều được quét virus và các phần mềm gián điệp. Ngoài việc quét dựa trên chữ ký cổ điển, phép phân tích heuristic cũng được sử dụng.

Một loạt các phương án chung cho quá trình quét cũng đươc hiện diện:

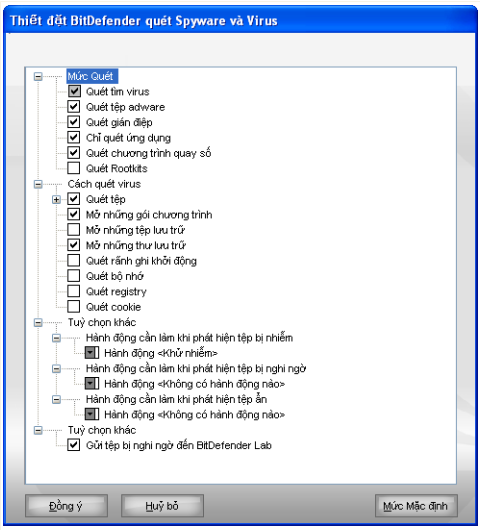
Phương án	Miêu tả
Vận hành nhiệm vụ có ưu tiên thấp	Giảm ưu tiên cho quá trình quét. Bạn sẽ cho phép các chương trình khác chạy nhanh hơn và tăng thời gian cần thiết để qúa trình quét kết thúc.
Mở cửa sổ quét ở mức tối thiểu khi khởi động ngăn hệ thống	Thu nhỏ cửa sổ quét vào khay hệ thống . Nhấp đúp vào biểu tượng BitDefender để mở.

Nhấp **OK** để lưu các thay đổi và đóng cửa sổ lại. Để tiến hành nhiệm vụ này, chỉ cần nhấp **Scan**.

Tùy biến mức quét

Những người dùng có trình độ cao có thể muốn tận dụng các lợi thế của các thiết lập quét do BitDefender cung cấp. Công cụ quét có thể được thiết lập chỉ để quét các phần mở rộng riêng, để tìm một loại malware đặc biệt hay bỏ qua tập tin nén. Việc này giảm đi đáng kể thời gian quét và cải thiện sự thích ứng của máy tính trong một lần quét.

Ấn **Tuỳ biến** để đặt các phương án quét của mình. Một cửa sổ mới sẽ xuất hiện:



Cài đặt quét

Các phương án quét được tổ chức giống như một thực đơn có thể mở rộng, rất giống với các phương pháp duyệt (exploring) của Windows. Nhấp vào hộp có "+" để mở một phương án hoặc vào hộp có "-" để đóng một phương án.

Các phương án quét được nhóm thành năm danh mục:

- **Cấp độ quét**
- **Các phương án quét virus**
- **Các phương án hành động**
- **Các phương án khác**

- Xác định kiểu của malware mà bạn muốn BitDefender quét bằng cách chọn các tùy chọn từ danh mục **Cấp độ quét**.

  Có những lựa chọn sau:

Phương án	*Miêu tả*
Quét Virus	Quét bộ nhớ để tìm virus đã biết.

Phương án	Miêu tả
	BitDefender phát hiện ra các thân virus chưa hoàn chỉnh, đồng thời gỡ bỏ các tác nhân có thể tác động xấu đến hệ thống bảo mật của bạn.
Quét adware	Quét adware. Những tập tin bị nhận diện sẽ được xử lý như những tập tin bị nhiễm. Phần mềm bao gồm các thành có chứa adware có thể bị ngừng làm việc nếu tùy chọn này được kích hoạt.
Quét Spyware	Quét những spyware đã biết. Tệp tin bị nhận diện sẽ bị coi như đã bị nhiễm.
Quét ứng dụng	Quét các ứng dụng (tệp tin `.exe` và `.dll`).
Quét dialers	Quét các ứng dụng quay số . Những tập tin bị nhận diện sẽ được xử lý như những tập tin bị nhiễm. Phần mềm bao gồm các thành phần quay số có thể ngừng bị ngừng hoạt động nếu tùy chọn này được kích hoạt.
Quét rootkits	Quét những đối tượng ẩn (tệp tin và tiến trình), được biết chung như là rootkits.

- Xác định rõ loại các đối tượng để quét (các tài liệu lưu trữ, thư điện tử.....) và các phương án khác. Việc này được tiến hành quan lựa chọn một số phương án nhất định từ phạm trù **Các phương án quét virus** category.

  Có những lựa chọn sau:

Phương án		Miêu tả
Quét các tập tin	**Quét tất cả các tập tin**	Tất cả các tập tin đã được truy cập sẽ được quét, bất kể chúng thuộc loại nào.
	Chỉ quét các tập tin chương trình	Chỉ có các tập tin chương trình sẽ được quét. Điều này có nghĩa là chỉ có các tập tin với những phần mở rộng sau: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`;

Phương án		Miêu tả
		smm; pdf; msi; ini; csc; cmd; bas; eml and nws.
	Quét các phần mở rộng do người sử dụng xác định	Chỉ các tập tin với những phần mở rộng do người sử dụng chỉ ra sẽ được quét. Những phần mở rộng này phải được tách ra bằng ";".
Mở các chương trình được đóng gói		Quét các tập tin được đóng gói.
Mở các phần lưu trữ		Quét bên trong các phần lưu trữ.
Mở các lưu trữ thư điện tử		Quét bên trong các lưu trữ thư điện tử.
Quét các rãnh ghi khởi động		Quét các rãnh ghi của hệ thống.
Quét bộ nhớ		Quét để tìm virus và các phần mềm nguy hiểm khác.
Quét đăng ký		Quét các lói vào để đăng ký.
Quét cookies		Quét các tập tin cookie.

- Xác định rõ hành động đối với các tập tin bị nhiễm, bị nghi ngờ hoặc các tập tin ẩn được nhận diện tại danh mục **Tùy chọn hành động**. Bạn có thể thiết lập các hành động khác nhau cho mỗi danh mục.
  - Chọn hành động để xử lý đối với tập tin bị lây nhiễm. Có những lựa chọn sau:

Hành động	Miêu tả
Không (Ghi lại các đối tượng)	Không có hành động nào được tiến hành đối với các tập tin bị lây nhiễm. Các tập tin này sẽ xuất hiện trong tập tin báo cáo.
Tẩy trùng cho các tập tin	Làm sạch tập tin bị nhiễm.
Xoá các tập tin	Xoá các tập tin bị nhiễm ngay lập tức, không cần cảnh báo.
Chuyển tập tin đến Kiểm dịchMove files to Quarantine	Chuyển các tập tin bị nhiễm đến Vùng cách ly.

  - Chọn hành động để xử lý đối với tập tin bị nghi ngờ. Có những lựa chọn sau:

Hành động	Miêu tả
Không (Ghi lại các đối tượng)	Không có hành động nào được tiến hành đối với các tập tin nghi ngờ. Các tập tin này sẽ có trong báo cáo.
Xoá các tập tin	Xoá các tập tin bị nghi ngờ ngay lập tức, không cần cảnh báo.
Chuyển tập tin đến Kiểm dịchMove files to Quarantine	Chuyển các tập tin bị nghi ngờ đến Vùng cách ly.

Ghi chú
Các tệp tin bị nghi ngờ bởi chương trình phân tích heuristic. Chúng tôi đề nghị bạn gửi các tệp tin trên đến BitDefender Lab.

- Chọn cách xử lí với những đối tượng ẩn (rootkits) bị phát hiện. Có những lựa chọn sau:

Hành động	Miêu tả
Không (Ghi lại các đối tượng)	Không có hành động nào được tiến hành đối với các tập tin ẩn. Các tập tin này sẽ xuất hiện trong báo cáo.
Chuyển tập tin đến Kiểm dịchMove files to Quarantine	Chuyển các tập tin ẩn đến Vùng cách ly.
Làm hiện	Phát hiện ra tập tin ẩn vì vậy bạn sẽ thấy chúng.

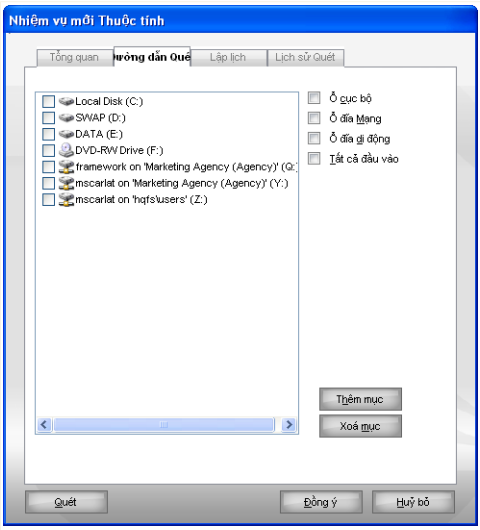
Ghi chú
Nếu như bạn chọn bỏ qua (ignore) những tập tin bị phát hiện ra hoặc nếu như việc chọn bị thất bạn, bạn sẽ phải chọn một hành động từ thuật sĩ.

- Để nhắc nhở việc gửi các tệp tin bị nghi ngờ đến BitDefender Lab sau khi quá trình quét hoàn thành, kiểm tra **Đư các tệp tin bị nghi ngờ đến BitDefender Lab** trong nhóm **Tùy chọn khác**.

Nếu bạn nhấp vào **Mặc định** bạn sẽ tải thiết lập mặc định. Nhấp **OK**để lưu lại các thay đổi và đóng cửa sổ lại.

Thiết lập mục tiêu quét

Để chỉ rõ mục tiêu quét của một nhiệm vụ nào đó, bạn chỉ cần nhấp chuột phải vào nhiệm vụ và chọn **Chọn Đường dẫn** . Cửa sổ kế tiếp hiện ra:



Mục tiêu quét

Bạn có thể nhìn thấy dễ dàng danh sách các ổ đĩa trong máy, ổ đĩa mạng, các ổ cắm ngoài như các tệp tin hoặc thư mục trước đây. Tất cả các chương trình đã được kiểm tra sẽ bị quét khi chạy các nhiệm vụ.

Phần này chứa các nút sau:

- **Thêm mục (Item)** - mở một cửa sổ duyệt qua tại đây bạn có thể chọn các tập tin / thư mục mà bạn muốn quét.

> ***Ghi chú***
> Bạn cũng có thể kéo lên hoặc kéo xuống để bổ sung thêm các tập tin/các thư mục.

- **Xóa các mục** - Loại bỏ các tập tin/ thư mục mà trước đây đã được chọn từ danh sách các đối tượng phải quét.

Ghi chú

Chỉ có các tập tin/các thư mục được chọn sau này mới có thể xoá bỏ được nhưng không phải đối với các tập tin/thư mục do BitDefender chọn "seen\.

Ngoài những nút được giải thích ở ttrên cũng còn có một số phương án cho phép lựa chọn nhanh các vị trí phải quét.

- **Các ổ đĩa nội bộ** - Để quét các ổ đĩa nội bộ.
- **Các ổ đĩa mạng** - Để quét các ổ đĩa mạng.
- **Các ổ đĩa lưu động** - Để quét các ổ đĩa lưu động (CD-ROM, đĩa mềm).
- **Tất cả** - để quét tất cả các ổ đĩa, cho dù chúng là ổ đĩa nội bộ, trong mạng hay ổ lưu động.

Ghi chú

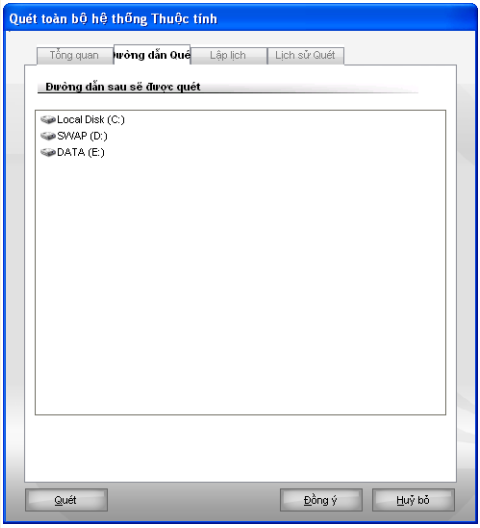
Nếu bạn muốn quét toàn bộ máy tính, hãy chọn hộp kiểm tra tương ứng là **Tất cả**.

Nhấp **OK** để lưu các thay đổi và đóng cửa sổ lại. Để tiến hành nhiệm vụ này, chỉ cần nhấp **Scan**.

Xem lại mục tiêu Quét của Nhiệm vụ Hệ thống

Để chỉ rõ mục tiêu quét của một nhiệm vụ nào đó, bạn chỉ cần nhấp chuột phải vào nhiệm vụ và chọn **Đường dẫn** . Bạn chỉ có thể xem mục tiêu quét.

Để chỉ rõ mục tiêu quét của một nhiệm vụ nào đó, bạn chỉ cần nhấp chuột phải vào nhiệm vụ và chọn **Hiện Đường dẫn** . Để **Quét toàn Hệ thống**, ví dụ, cửa sổ sau sẽ hiện ra:



Quét mục tiêu Toàn bộ Hệ thống

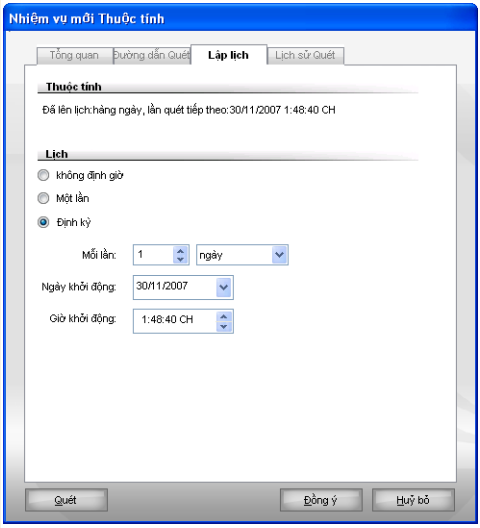
Quét Toàn bộ Hệ thống và **Quét Sâu Hệ thống** sẽ quét tất cả ổ đĩa của máy, trong khi **Quét nhanh Hệ thống** chỉ quét `Windows` và mục `Program Files`.

Nhấp **OK**để đóng cửa sổ lại. Để chạy nhiệm vụ, ấn **Quét**.

Lên kế hoạc các nhiệm vụ quét

Với các nhiệm vụ phức tạp, quá trình quét sẽ phải mất một số thời gian và sẽ hoạt động tốt nhất khi bạn đóng tất cả các chương trình khác. Đó là lý do tại sao bạn phải lên kế hoạch cho các nhiệm vụ như vậy khi bạn không sử dụng máy tính của bạn và nó sẽ đi vào chế độ để không dùng đến.

Để xem hoặc chỉnh sửa kế hoạch của một nhiệm vụ cụ thể, bạn chỉ cần nhấp chuột phải vào đó và chọn **Kế hoạch**. Cửa sổ kế tiếp hiện ra:



Lập lịch trình

Bạn có thể xem kế hoạch của nhiệm vụ.

Khi lên kế hoạch cho một nhiệm vụ, bạn phải chọn một trong các phương án sau:

- **Không được lên kế hoạch** -Khởi động nhiệm vụ chỉ khi nào có yêu cầu của người sử dụng.
- **Once** -Bắt đầu quét chỉ một lần tại một thời điểm nhất định. Nêu cụ thể ngày tháng và thời gian bắt đầu tại các trường **Ngày tháng bắt đầu /Thời gian**.
- **Định kỳ** - Khởi động quét định kỳ, trong những khoảng thời gian nhất định (Các giờ, các ngày, các tháng, các năm), bắt đầu với ngày, giờ cụ thể.

  Nếu bạn muốn quét lại vào những khoảng thời gian nhất định nào đó, hãy chọn **Periodically** và đánh **vào mỗi** hộp hiệu chỉnh số phút/giờ/ngày/tuần/tháng/năm,, chỉ tần suất của quá trình này. Bạn cũng phải nêu rõ ngày, giờ bắt đầu trên các trường **Start Date/Time**.

Nhấp **OK** để lưu các thay đổi và đóng cửa sổ lại. Để tiến hành nhiệm vụ này, chỉ cần nhấp **Scan**.

7.2.5. Nội dung quét

Trước khi bạn bắt đầu một quá trình quét, bạn nên chắc chắn rằng BitDefender được cập nhật mới nhất các loại maiware. Việc quét máy tính của bạn với một cơ sở dữ liệu đã quá cũ thì BitDefender sẽ chỉ nhận ra được các loại malware cũ được cập nhật từ lần cập nhật trước. Để kiểm tra khi lần cập nhật mới nhất được thi hành, ấn vào **Update>Update** trong bảng điều khiển thiết lập.

Ghi chú

Để cho BitDefender hoàn tất việc quét, bạn cần phải đóng tất cả các chương trình đang mở. Đặc biệt là chương trình thư điện tử của bạn (như. Outlook, Outlook Express or Eudora) rất cần phải đóng lại.

Phương thức quét

BitDefender cho phép bốn kiểu quét theo yêu cầu:

- Quét ngay lập tức - vận hành một nhiệm vụ quét từ hệ thống / các nhiệm vụ của người sử dụng.
- Quét theo bối cảnh - nhận chuột phải vào một tập tin hoặc một thư mục và lựa chọn BitDefender Antivirus 2008;
- Kéo& thả khi quét - kéo và thả một tập tin hoặc một thư mục trên Thanh hoạt động Quét;
- Quét thủ công - sử dụng BitDefender Manual Scan để trực tiếp chọn tệp tin hoặc thư mục muốn quét.

Quét ngay lập tức

Để quét toàn bộ hoặc một phần của máy tính, bạn có thể sử dụng các nhiệm vụ quét mặc định hoặc bạn có thể tự tạo ra các nhiệm vụ quét của mình. Quét ngay lập tức.

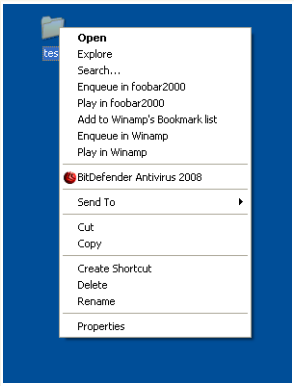
Để chạy một hành động quét, chọn một trong các phương thức sau đây:

- Click đôi vào công tác quét trong danh sách.
- Hãy nhấn nút **Quét ngay** tương ứng.
- Chọn nhiệm vụ và nhấn **Chạy nhiệm vụ**.

BitDefender Scanner sẽ xuất hiện và sẽ bắt đầu quét. Để có thêm thông tin, hãy chuyển đến “*BitDefender Scanner*” (p. 64).

Quét theo bối cảnh

Để quét một file hoặc một thư mục, ngoài việc tinh chỉnh mới công tác quét, bạn có thể sử dụng trình đơn ngữ cảnh. Quét theo ngữ cảnh.



Quét theo bối cảnh

Nhấp chuột phải vào tập tin hoặc thư mục bạn muốn quét và chọn **BitDefender Antivirus 2008**.

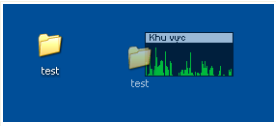
BitDefender Scanner sẽ xuất hiện và sẽ bắt đầu quét. Để có thêm thông tin, hãy chuyển đến "*BitDefender Scanner*" (p. 64).

Bạn có thể sửa đổi các tùy chọn quét và xem các tập tin báo cáo bằng cách truy cập vào cửa sổ **Thuộc tính** của nhiệm vụ **Thực đơn quét ngữ cảnh**.

Quét kéo và thả

Kéo tập tin hoặc thư mục bạn muốn quét và thả chúng xuống trên **Thanh Hoạt động quét** như được mô tả dưới đây.

Kéo tập tin



Thả tập tin

BitDefender Scanner sẽ xuất hiện và sẽ bắt đầu quét. Để có thêm thông tin, hãy chuyển đến “*BitDefender Scanner*” (p. 64).

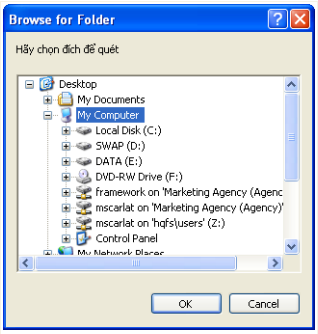
Quét thủ công

Quét bằng tay (Manual Scanning) thực chất là trực tiếp chọn các đối tượng cần quét. Sử dụng tùy chọn BitDefender Manual Scan từ thư mục BitDefender trong Start Menu.

> ***Ghi chú***
> Quét bằng tay rất hữu dụng, nó có thể chạy ngay cả khi Windows chạy trong chế độ Safe Mode.

Để chọn các đối tượng được quét bởi BitDefender, ở trình đơn Start của Windows, hãy theo đường dẫn **Start → Programs → BitDefender 2008 → BitDefender Manual Scan**.

Cửa sổ kế tiếp hiện ra:



Quét thủ công

Chọn đối tượng muốn quét và nhấn **Đồng ý**.

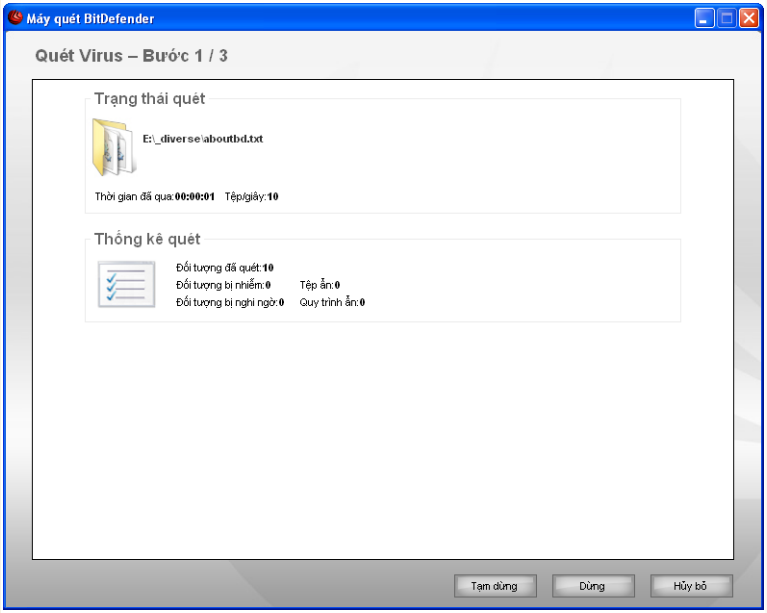
BitDefender Scanner sẽ xuất hiện và sẽ bắt đầu quét. Để có thêm thông tin, hãy chuyển đến “*BitDefender Scanner*” (p. 64).

BitDefender Scanner

Khi bạn bắt đầu một quá trình quét theo yêu cầu, Máy quét BitDefender sẽ xuất hiện. Làm theo qui trình 3 bước có hướng dẫn để hoàn thành quá trình quét

Bước 1/3 - Đang quét

BitDefender sẽ bắt đầu quét những đối tượng được chọn



Đang quét

Bạn có thể xem thấy tình trạng quét và các thống kê (tốc độ quét, thời gian đã quét, số các đối tượng được quét/bị nhiễm/nghi ngờ...).

Ghi chú
Quá trình quét có thể mất một lhoảng thời gian, tuỳ thuộc vào độ phức tạp của lần quét.

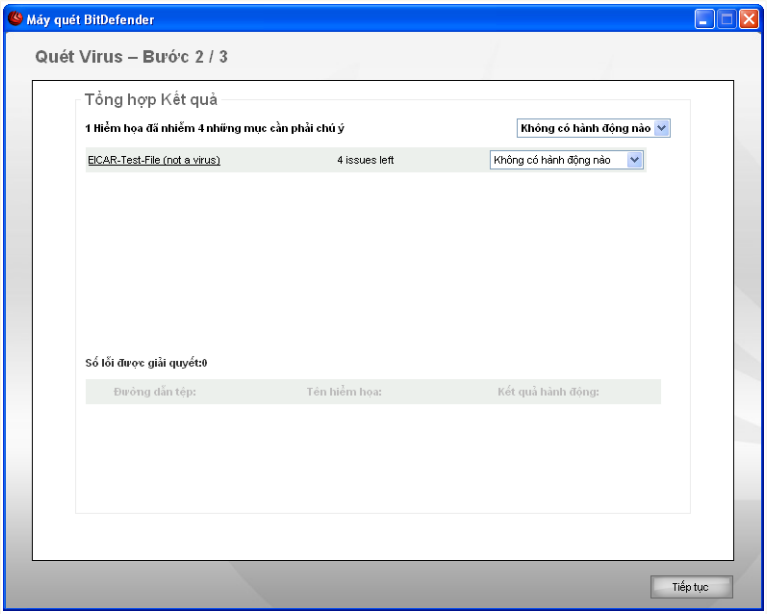
Để tạm thời ngừng quá trình quét, chỉ việc ấn **Tạm dừng**. Bạn sẽ phải ấn **Khôi phục** để khôi phục lại quá trình quét.

Bạn có thể ngừng quá trình quét bất cứ khi nào bạn muốn bằng cách ấn **&Dừng**. Bạn sẽ chuyển đến bước cuối cùng của quá trình trợ giúp (wizard).

Chờ cho BitDenfender hoàn tất quá trình quét.

Bước 2/3 - Chọn cách thực hiện

Khi quá trình quét đã hoàn thành, một cửa sổ mới sẽ xuất hiện, nơi bạn có thể xem kết quả quét.



Hành động

Bạn có thể xem một số ảnh hưởng đến máy tính của bạn.

Những đối tượng bị nhiễm hiển thị theo nhóm, trên cơ sở malware gây nhiễm. Click link tương ứng với hiểm họa để tìm thông tin về những đối tượng bị nhiễm.

Bạn có thể chọn một hành động toàn diện cho mỗi nhóm vấn đề hoặc bạn cũng có thể tách riêng từng hành động cho mỗi vấn đề.

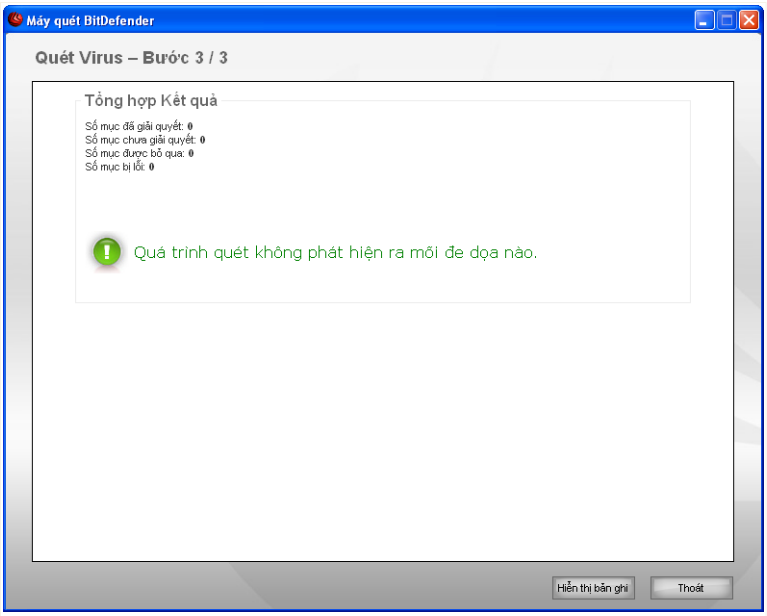
Các tùy chọn trên có thể xuất hiện ở trình đơn:

Hành động	Miêu tả
Không thực thi	Không có hành động nào được tiến hành đối với các tập tin đã nhận diện.
Loại bỏ mã độc	Làm sạch tập tin bị nhiễm.
Xoá	Xóa những tệp tin đã nhận diện.
Bỏ ẩn	Làm hiện các đối tượng đang ẩn.

Nhấn **Tiếp** để áp dụng hành động đã định.

Bước 3/3 - Xem kết quả

Khi BitDenferder kết thúc quá trình sửa vấn đề, kết quả quét sẽ xuất hiện ở một cửa sổ mới



Tổng kết

Bạn có thể xem bảng tổng hợp kết quả.

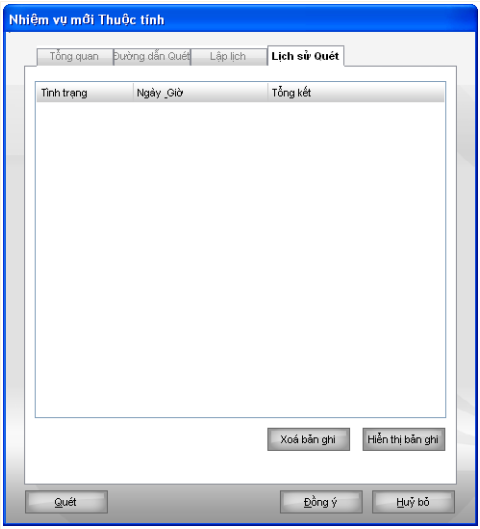
Nếu như những tệp tin bị nghi ngờ được tìm thấy trong quá trình quét, bạn sẽ được yêu cầu gửi chúng đến BitDefender Lab. File nghi vấn được phát hiện bởi phân tích hành vi và chúng có thể nhiễm với chữ ký mã độc mới mà chưa được biết tới.

Tập tin báo cáo sẽ tự động được lưu trong phần Nhật kí hệ thống từ cửa sổ **Thuộc tính** của nhiệm vụ tương ứng.

Cảnh báo
Nếu như có những vấn đề chưa giải quyết được, chúng tôi khuyến cáo bạn nên liên lạc với BitDefender Support Team tại www.bitdefender.com.

7.2.6. Xem nhật kí quét

Khi bạn muốn xem kết quả sau khi quét, bạn chỉ cần nhấp chuột phải vào đó và chọn **Nhật kí**. Cửa sổ kế tiếp hiện ra:



Quét các bản ghi

Tại đây bạn có thể thấy file báo cáo mỗi lần khi nhiệm vụ được hoàn thành

Mỗi tập tin có đính kèm các thông tin về tình trạng quét, ngày, giờ lúc việc quét được thực hiện và tóm tắt kết quả quét.

Có hai nút:

- **Xoá bản ghi** - để xoá bản ghi (scan log) được chọn.
- **Hiện bản ghi** - để xem bản ghi (scan log) được lựa chọn; Bản ghi (scan log) sẽ mở trong trình duyệt web.

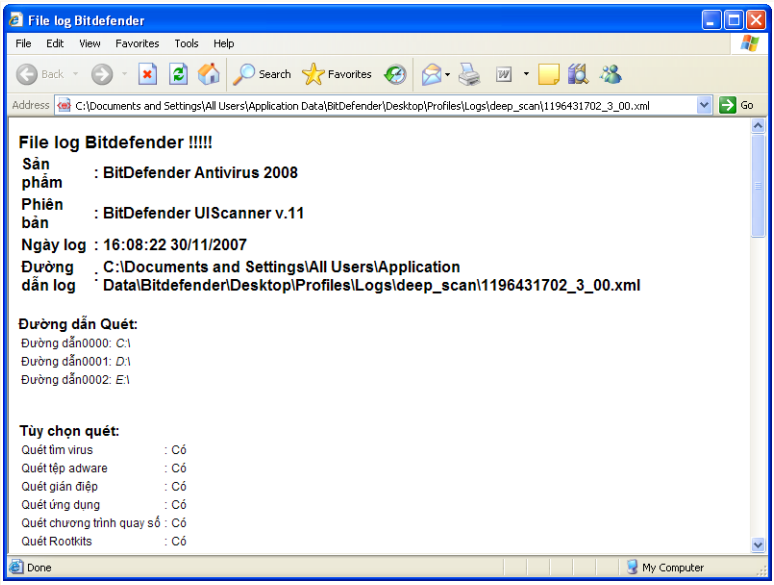
Ghi chú

Và cũng để xem hoặc xoá một tập tin, nhấp chuột phải vào tập tin và chọn phương án phù hợp từ thực đơn tắt.

Nhấp **OK** để lưu các thay đổi và đóng cửa sổ lại. Để tiến hành nhiệm vụ này, chỉ cần nhấp **Scan**.

Ví dụ Bản ghi Quét

Hình sau đây minh họa ví dụ bản ghi (scan log):



Ví dụ Bản ghi Quét

Bản ghi (Scan log) chứa thông tin chi tiết về quá trình quét, như là lựa chọn quét, đích quét, hiểm họa thấy được và hành động dã thực hiện.

7.3. Các đối tượng không được quét

Có một số trường hợp khi bạn cần loại bỏ một số tệp tin khỏi quá trình quét. Ví dụ, bạn muốn loại bỏ kiểm tra tệp tin EICAR từ việc quét truy cập hoặc tệp tin `.avi` khi quét theo yêu cầu.

BitDefender cho phép loại bỏ các đối tượng từ quá trình quét khi truy cập hay theo yêu cầu, hoặc cả hai. Chức năng này có tác dụng làm giảm thời gian quét và tránh mọi sự phiền toái khi bạn làm việc.

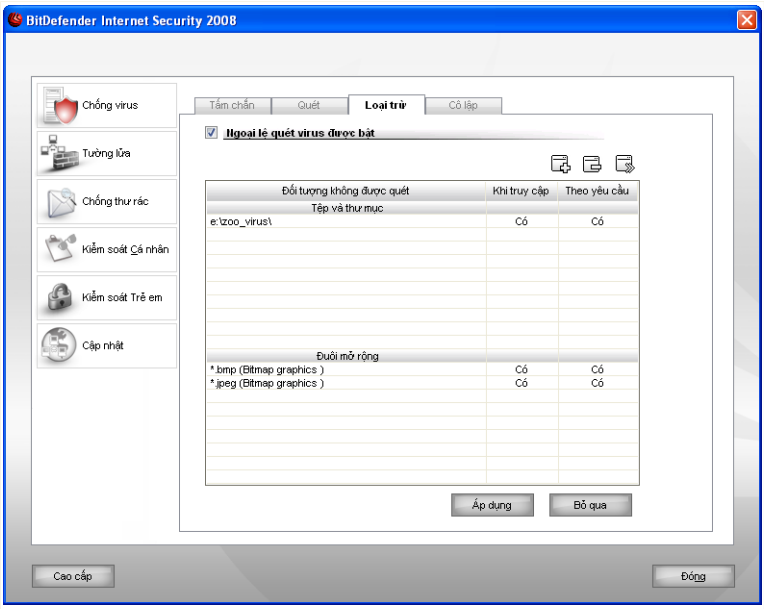
Hai loại của đối tượng có thể bỏ qua từ quá trình quét:

- **Đường dẫn** - của thư mục hoặc tệp tin (bao gồm tất cả các đối tượng trong nó) được chỉ ra bằng một đường dẫn đặc biệt sẽ được bỏ qua khi quét.
- **Phần mở rộng** - tất cả các tập tin có phần mở rộng đặc biệt sẽ được bỏ qua khi quét.

Ghi chú

Các đối tượng được bỏ qua trong quá trình quét khi truy cập sẽ không bị quét, sẽ không xảy ra chuyện gì nếu bạn hoặc có chương trình khác sử dụng chúng.

Để xem và quản lý những đối tượng ngăn chặn khỏi việc quét, kích chuột vào **Antivirus>Exceptions (Ngoại lệ)** trong hệ thống setting Cửa sổ kế tiếp hiện ra:



Ngoại trừ

Bạn có thể biết các đối tượng (tệp tin, thư mục, phần mở rộng) đã được bỏ qua khi quét. Với mỗi đối tượng, bạn có thể biết nếu nó được bỏ qua trong quá trình quét nào: quét theo yêu cầu, quét khi truy cập hay cả hai.

Ghi chú

Tại đây có một ngoại lệ đặc biệt sẽ KHÔNG áp dụng cho một quá trình quét ngữ cảnh(contextual)

Để xóa một mục từ bảng, hãy chọn và bấm vào nút **Xóa**.

Để sửa một mục trong bảng, hãy chọn và bấm vào nút **Xóa**. Một cửa sổ mới sẽ xuất hiện khi bạn thay đổi phần mở rộng hoặc đường dẫn và kiểu quét mà bạn muốn chúng được bỏ qua. Hãy thực hiện các thay đổi và ấn **Đồng ý**.

Ghi chú

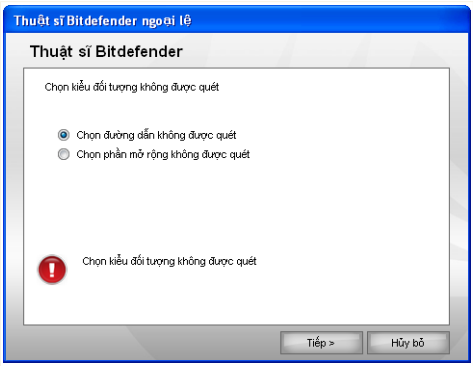
Bạn cũng có thể ấn phải chuột vào đối tượng và sử dụng tùy chọn trong trình đơn tắt để sửa hoặc xóa nó.

Nhấp **Bỏ qua** để không thay đổi bảng quy tắc, cho biết rằng bạn không lưu chúng bằng cách nhấn **Áp dụng**.

7.3.1. Đường dẫn được bỏ qua

Để bỏ qua các đường dẫn khi quét, nhấn vào nút **Thêm**. Bạn sẽ được chỉ dẫn xuyên suốt quá trình bỏ qua các đường dẫn khi quét bằng cách dùng trợ giúp cấu hình tự động.

Bước 1/3 - Chọn kiểu đối tượng

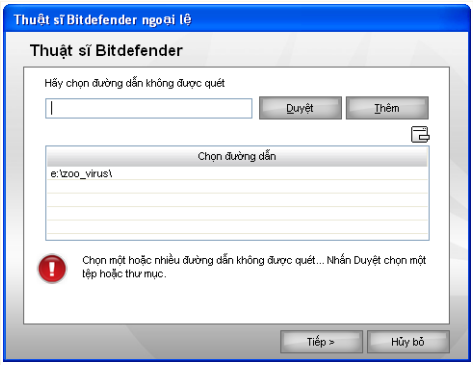


Kiểu đối tượng

Lựa chọn tùy chọn ngăn chặn một đường dẫn trong lúc quét.

Nhấp chuột vào **Next**.

Bước 2/3 – Xác định đường dẫn được bỏ qua



Đường dẫn được bỏ qua

Để đánh dấu các đường dẫn được bỏ qua khi quét sử dụng một trong hai phương pháp sau:

- Nhấn **Duyệ)**, chọn tệp tin hoặc thư mục bạn muốn bỏ qua trong khi quét và nhấn **Thêm**.
- Gõ đường dẫn mà bạn muốn bỏ qua khi quét vào trong trường chỉnh sửa và ấn **Thêm**.

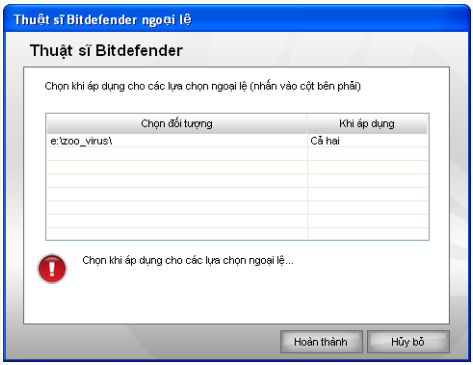
> ***Ghi chú***
> Nếu đường dẫn thêm vào không tồn tại, một hộp thoại báo lỗi sẽ xuất hiện. Ấn **Đồng ý** và kiểm tra lại đường dẫn.

Các đường dẫn sẽ xuất hiện trong bảng khi bạn thêm vào. Bạn có thể thêm bao nhiêu đường dẫn tùy ý.

Để xóa một mục từ bảng, hãy chọn và bấm vào nút **Xóa**.

Nhấp chuột vào **Next**.

Bước 3/3 - Chọn kiểu quét



Kiểu quét

Bạn có thể thấy một bảng có chứa các đường dẫn được bỏ qua khi quét và kiểu quét mà chúng được bỏ qua.

Mặc định, các đường dẫn đã chọn được bỏ qua với cả hai kiểu quét. Để thay đổi khi áp dụng cho các trường hợp riêng, ấn vào cột bên phải và chọn các tùy chọn có sẵn từ danh sách.

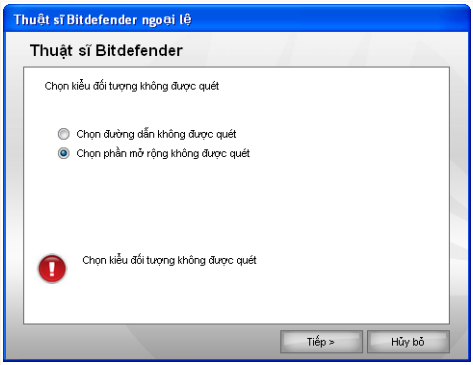
Nhấp vào **Kết thúc**.

Nhấn**Apply(áp dụng)** để lưu sự thay đổi.

7.3.2. Các phần mở rộng được bỏ qua

Để bỏ qua các phần mở rộng khi quét, nhấn nút **Thêm**. Bạn sẽ được chỉ dẫn xuyên suốt quá trình bỏ qua các phần mở rộng khi quét bằng cách dùng trợ giúp cấu hình tự động.

Bước 1/3 - Chọn kiểu đối tượng

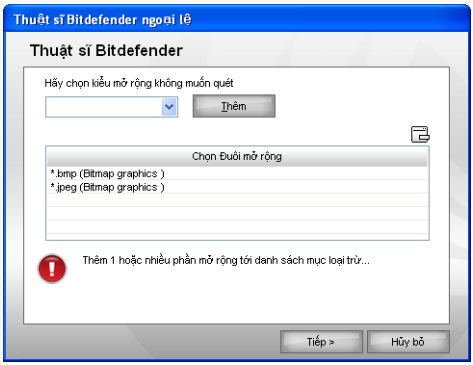


Kiểu đối tượng

Chọn các tùy chọn của các phần mở rộng được bỏ qua khi quét.

Nhấp chuột vào **Next**.

Bước 2/3 – Phần mở rộng được bỏ qua



Phần mở rộng được bỏ qua

Để đánh dấu các phần mở rộng được bỏ qua khi quét sử dụng một trong hai phương pháp sau:

- Chọn từ trình đơn các phần mở rộng bạn muốn bỏ qua khi quét và ấn **Thêm**.

> ***Ghi chú***
> Trình đơn bao gồm một danh sách tất cả các phần mở rộng đã được đăng kí trong hệ thống của bạn. Khi bạn chọn một phần mở rộng, bạn sẽ thấy các thông tin mô tả của nó nếu tồn tại.

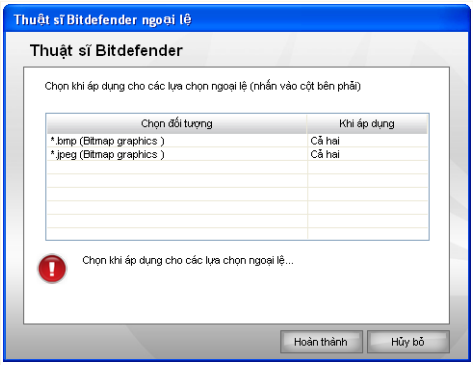
- Nhập phần mở rộng bạn muốn bỏ qua trong quá trình quét và nhấp **Thêm**.

Các phần mở rộng sẽ xuất hiện trong bảng khi bạn thêm vào. Bạn có thể thêm bao nhiêu tùy ý.

Để xóa một mục từ bảng, hãy chọn và bấm vào nút **Xóa**.

Nhấp chuột vào **Next**.

Bước 3/3 - Chọn kiểu quét



Kiểu quét

Bạn có thể thấy một bảng có chứa các phần mở rộng được bỏ qua khi quét và kiểu quét mà chúng được bỏ qua.

Mặc định, các phần mở rộng đã chọn được bỏ qua với cả hai kiểu quét. Để thay đổi khi áp dụng cho các trường hợp riêng, ấn vào cột bên phải và chọn các tùy chọn có sẵn từ danh sách.

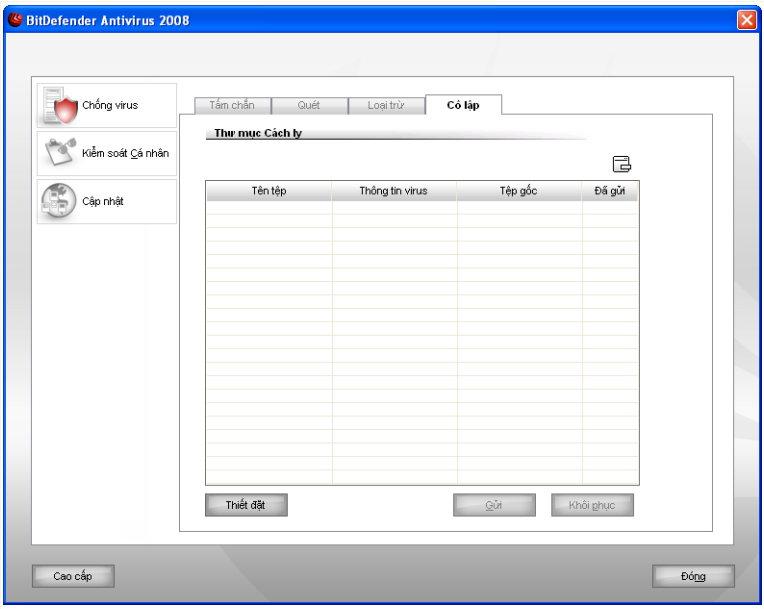
Nhấp vào **Kết thúc**.

Nhấn**Apply(áp dụng)** để lưu sự thay đổi.

7.4. Vùng cách ly

BitDefender cho phép cách ly các tập tin bị nhiễm hay bị nghi ngờ trong một vùng an toàn, gọi là khu kiểm dịch. Bằng cách cô lập các tệp này trong Vùng cách ly, nguy phát tán mã độc sẽ mất đi, đồng thời bạn có khả năng gửi các tệp tin này tới phòng thí nghiệm của BitDefender để phân tích tiếp.

Để thấy và quản lý các tệp tin đac được cách ly và cấu hình các thiết lập cách ly, ấn vào **Antivirus>Quarantine** trong bảng điều khiển thiết lập.



Cách ly

7.4.1. Quản lý những tệp tin đang chờ cách ly

Như bạn được nhắc nhở, phần **Cách ly** chứa một danh sách tất cả các tập tin được cách ly từ trước tới nay. Mỗi một tập tin đều có kèm tên, kích cỡ, tên virus bị nhiễm, đường dẫn tới vùng chứa nó và ngày xác nhận.

Ghi chú

Khi virus được cách ly, chúng sẽ không thể tạo được tác hại nào nữa bởi vì chúng sẽ không còn có thể đọc được cũng như không thể thực thi được các nhiệm vụ nữa.

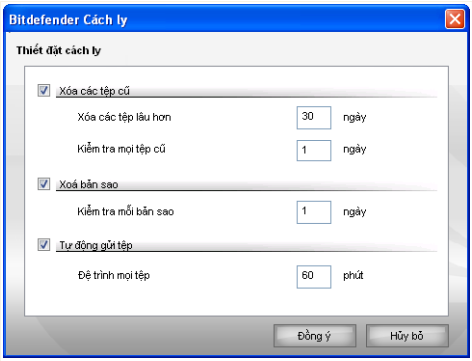
Để xoá một tập tin được chọn lựa từ Vùng cách ly, hãy nhấp vào nút **Xóa**. Nếu bạn muốn khôi phục lại một tập tin được chọn trở lại vị trí ban đầu của nó thì nhấp vào **Khôi phục**.

Bạn có thể gửi bất cứ tập tin nào từ vùng kiểm dịch đến phòng thí nghiệm của BitDefender bằng cách nhấp vào **Gửi**.

Trình đơn ngữ cảnh. Một menu hoàn cảnh tồn tại, cho phép bạn quản lý các tệp tin bị cách ly dễ dàng. Tùy chọn tương tự các đề cập trên cũng tồn tại. Bạn cũng có thể chọn **Refresh** để làm mới Vùng cách ly.

7.4.2. Cấu hình thiết lập Vùng cách ly

Để cấu hình các thiết lập của Vùng cách ly, nhấn **Thiết lập**. Một cửa sổ mới sẽ được hiện ra



Thiết lập Cách ly

Sử dụng các thiết lập cách ly, bạn có thể thiết lập BitDefender tự động tiến hành theo các bước sau:

Xóa những File cũ. Để tự động xóa những tệp bị cách ly cũ, tích tùy chọn tương ứng. Bạn phải đưa ra số ngày mà các tệp tin bị cách ly cần được xóa và tần suất mà BitDefender nên kiểm tra các tệp tin cũ.

Ghi chú
Mặc định, BitDenfender sẽ kiểm tra các tập tin cũ mỗi ngày và xóa chúng khi đã hơn 10 ngày.

Xóa những tệp tin trùng. Để tự động xóa những tập tin cách ly bị trùng, hãy chọn tùy chọn tương ứng. Bạn phải chỉ định rõ số ngày giữa 2 lần kiểm tra liên tiếp cho những tập tin trùng

Ghi chú
Mặc định, BitDenfender sẽ kiểm tra các tập tin cũ mỗi ngày và xóa chúng khi đã hơn 10 ngày.

Tự động xem xét tập tin. Để tự động gửi những tập tin cách ly, hãy chọn tùy chọn tương ứng. Bạn phải chỉ rõ tần số đối với các tệp tin đã được kiểm tra.

Ghi chú
Mặc định, BitDefender sẽ tự động chuyển vào vùng cách ly sau mỗi 60 phút.

Nhấp **OK**để lưu lại các thay đổi và đóng cửa sổ lại.

8. Kiểm soát riêng tư

BitDefender theo dõi hàng chục "điểm nóng" tiềm tàng trong hệ thống của bạn, những nơi mà chương trình gián điệp có thể hoạt động và cũng kiểm tra luôn bất cứ thay đổi nào trong hệ thống và phần mềm của bạn. Nó hiệu quả trong việc chặn đứng các "Con ngựa thành Trojan" và các công cụ khác do hackers cài đặt hòng cố gắng xâm nhập các bí mật cá nhân của bạn và gửi đi thông tin cá nhân của bạn như số thẻ tín dụng từ máy tính của bạn cho hacker.

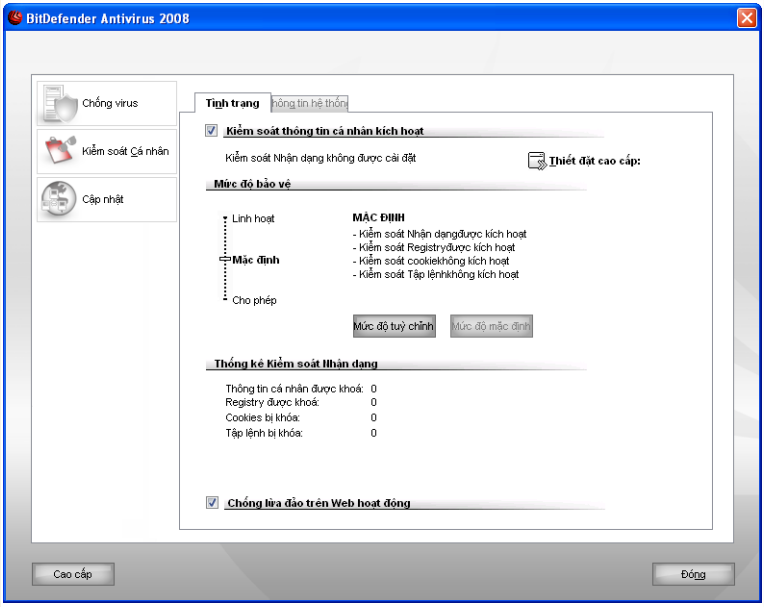
BitDefender có thể quyets những website bạn ghé thăm và cảnh báo bạn nếu như có một nguy cơ lừa đảo nào đó được phát hiện.

Mục**Kiểm soát trẻ em** của cuốn sách hướng dẫn sử dụng này bao gồm các chủ đề sau:

- Trạng thái kiểm soát nhận diện
- Cài đặt cấp cao - Kiểm soát riêng tư
- Cài đặt cấp cao-Kiểm soát đăng ký sản phẩm
- Cài đặt cấp cao-Kiểm soát cookie
- Cài đặt cấp cao-kiểm soát tập lệnh
- thông tin hệ thống
- Thanh công cụ Antiphishing

8.1. Kiểm soát riêng tư

Để cấu hình Nhận dạng Điều khiển và hiển thị thông tin lưu ý đến các hoạt động của nó, ấn **Trạng thái>Điều khiển Nhận dạng** Cửa sổ kế tiếp hiện ra:



Kiểm soát riêng tư

8.1.1. Kiểm soát riêng tư

Quan trọng

Để ngăn trộm cắp và bảo mật cho máy tính của bạn được **Kiểm soát Riêng tư**được kích hoạt.

Identity Control bảo vệ máy tính của bạn bằng cách sử dụng 5 kiểm soát bảo vệ quan trọng:

- kiểm soát riêng tư - bảo vệ những dữ liệu riêng tư của bạn bằng cách lọc tất cả những giao dịch ra HTTP và SMTP theo những qui tắc bạn đã đặt trong phần Riêng tư.

Ghi chú

Tại cuối đoạn bạn có thể thấy**Thống kê kiểm soát nhận dạng**.

- Kiểm soát Registry - hỏi bạn có cho phép một chương trình thay đổi registry để hoạt động trong Windows start-up.
- Kiểm soát Cookie - hỏi bạn có cho phép một website mới muốn ghi vào cookie.
- Kiểm soát Script - hỏi bạn có cho phép một website muốn khởi động script hoặc bất cứ active content nào.

Để cấu hình cho những kiểm soát này nhấn Cấu hình cao cấp.

Cấu hình cấp độ bảo vệ

Bạn có thể chọn mức bảo vệ phù hợp hơn với các yêu cầu an ninh của bạn. Hãy kéo thanh trượt dọc theo mặt chia độ để chọn mức bảo vệ phù hợp.

Có 3 mức bảo vệ:

Mức bảo vệ	Miêu tả
Được chấp nhận	Chỉ khi **Kiểm soát Registry** hoạt động.
Mặc định	**Kiểm soát Registry** và **Kiểm soát quay điện thoại** đang hoạt động.
Tấn công	**Kiểm soát Registry**, **Kiểm soát TT cá nhân** và **Kiểm soát gói mã** đã kích hoạt.

Bạn có thể tuỳ chỉnh mức an toàn bằng cách nhấp chuột vào **Mức tự chọn**. Trong cửa sổ sẽ hiện ra, hãy chọn hình thức bảo vệ và nhấn **OK**.

Nhấp **Mức mặc định** để đặt con trượt vào mức mặc định.

8.1.2. Bảo vệ khỏi Antiphishing

Phishing (lừa đảo) là một hoạt động lừa đảo trên mạng Internet mà sử dụng những công nghệ kiến thức về xã hội để lừa đảo mọi người đưa ra những thông tin cá nhân/mật của họ.

Đa số, những tên lừa đảo thường cố gắng gửi rất nhiều e-mail giả mạo như là được gửi từ một doanh nghiệp hợp pháp và đã được xác minh. Những bức thư lừa bịp này được gửi đi với hi vọng rằng có ít nhất một vài người nhận sẽ phù hợp với thông tin mà bọn lừa đảo nhắm tới được thuyết phục để lộ ra những thông tin cá nhân/mật.

Một bức thư lừa đảo thường xuất hiện với một thông tin liên quan đến tài khoản trực tuyến của bạn. Nó cố gắng để thuyết phục bạn nhấn vào một đường dẫn kèm theo trong bức thư để truy cập vào một trang web được cho là hợp pháp (mà thật sự là,

chỉ là giả mạo) nơi mà thông tin cá nhân/mật đòi hòi. Bạn có thể được hỏi, ví dụ như là, xác nhận lại thông tin về tài khoản, như là tên truy cập và mật khẩu hay tài khoản ngân hàng. Đôi khi, để cho thuyết phục hơn, bức thư có thể giả vờ làm như là tài khoản của bạn đã bị hoặc có khả năng bị đóng cửa nếu như bạn không sử dụng đường dẫn kèm theo.

Những tên lừa đảo thường sử dụng phần mềm gián điệp, như là Trojan keyloggers, để đánh cắp thông tin về tài khoản ngay chính từ máy tính của bạn.

Đối tượng mà bọn lừa đảo thường nhắm đến là khách hàng của những dịch vụ trả tiền trực tuyến, như là eBay và PayPal, cũng như là các ngân hàng cung cấp các dịch vụ trực tuyến Gần đây, thành viên của các website mạng lưới xã hội cũng là mục tiêu của các dạng lừa đảo nhằm lấy thông tin nhận dạng cá nhân để dùng cho việc đánh cắp nhân dạng.

Để được bảo vệ khỏi sự tấn công của các phishing khi bạn kết nối Internet, hãy giữ **Antiphishing** luôn kích hoạt. BitDefender sẽ quét từng website trước khi bạn truy cập nó và chương trình sẽ cảnh báo bạn về sự hiện diện của bất cứ hiểm họa lừa đảo nào. Một Sổ Trắng những website mà không được quét bởi BitDefender có thể được cấu hình.

Nhằm mục đích dễ quản lý việc phòng tránh lừa đảo và Sổ Trắng, sử dụng thanh công cụ BitDefender Antiphishing được tích hợp vào IE. Để biết thêm thông tin, hãy chuyển đến “*Thanh công Antiphishing*” (p. 100).

8.2. Cài đặt cấp cao - Kiểm soát Registry

Giữ những dữ liệu an toàn bí mật là một vấn đề rất quan trọng mà ai cũng quan tâm. Những kẻ cắp dữ liệu luôn song hành với sự phát triển của Internet và sử dụng những công nghệ mới nhất để lừa người sử dụng vô tình đưa số liệu co chúng.

Bất kể địa chỉ e-mail của bạn hay số thẻ tín dụng, khi nó rơi vào tay kẻ xấu thì nó có thể huỷ hoại bạn: bạ sẽc nhận được không biết bao nhiêu thư rác hoặc bạn sẽ bất ngờ thấy tài khoản của bạn trống rỗng.

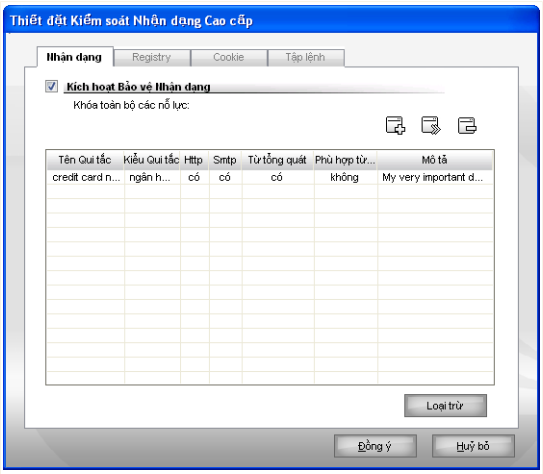
Kiểm soát riêng tư giúp bạn giữ dữ liệu của bạn an toàn. Nó quét những giao dịch HTTP hoặc SMTP, hoặc cả hai, tìm những đoạn viết mà bạn đã định nghĩa. nếu thấy, những trang web hoặc e-mail sẽ bị ngăn chặn.

Hỗ trợ đa người dùng được cung cấp vì thế không có người dùng khác trong hệ thống có thể thấy được những quy định mà bạn đã cấu hình.

Các quy tắc cá nhân có thể được cấu hình trong mục **Cá nhân**. Để truy xuất vào phần này, mở cửa sổ **Thiết lập kiểm soát TT cá nhân nâng cao** và chọn thẻ **Registry**.

Ghi chú

Để mở cửa sổ **Thiết lập kiểm soát nhận dạng nâng cao** , nhấn **Trạng thái kiểm>soát cá nhân** trong bảng điều khiển thiết lập và ấn **Thiết lập nâng cao**.



Kiểm soát Thông tin cá nhân

8.2.1. Tạo nguyên tắc cá nhân

Những qui tắc cần được thiết lập một cách thủ công (Nhấp nút **Thêm** và chọn các thông số của qui tắc. Cửa sổ thuật sĩ cài đặt sẽ được mở ra.

Thuật sĩ cài đặt rút lại còn 3 bước.

Bước 1/3 - Cài Loại Qui tắc và Dữ liệu

Cài Loại Qui tắc và Dữ liệu

Vào tên của qui tắc trong trường được sửa.

Bạn cần phải cài đặt những thông số sau:

- **Loại Qui tắc** - chọn loại qui tắc (địa chỉ, tên, thẻ tín dụng, PIN, SSN v.v...).
- **Dữ liệu Qui tắc** - vào trong Dữ liệu Qui tắc.

> ***Ghi chú***
> Nếu như bạn nhập vào ít hơn 3 ký tự, bạn sẽ phải nhắc là kiểm tra lại thông tin. Chúng tôi khuyến cáo bạn phải nhập vào ít nhất 3 ký tự để tránh việc ngăn chặn nhầm tin nhắn hoặc trang web.

Tất cả các dữ liệu bạn đưa vào đề được mã hoá. Để an toàn hơn, đừng nên đưa toàn bộ những dữ liệu vào bảo vệ.

Nhấp chuột vào **Next**.

Bước 2/3 - Chọn Giao dịch

Chọn Giao dịch

Chọn kiểu giao dịch mà bạn muốn BitDefender sẽ quét. Có những lựa chọn sau:

- **Quét HTML** - Quét giao dịch HTML (web) và ngăn chặn dữ liệu ra ngoài theo qui tắc được đặt.
- **Quét SMTP** - quét giao dịch SMTP (mail) và ngăn chặn những tin nhắn e-mail trong dữ liệu qui tắc.

Bạn có thể chọn áp dụng quy tắc nếu như dữ liệu quy tắc phù hợp với toàn bộ từ hoặc nếu như dữ liệu quy tắc và chuỗi được tìm thấy phù hợp với nhau

Nhấp chuột vào **Next**.

Bước 3/3 - Mô tả Qui tắc

Mô tả Qui tắc

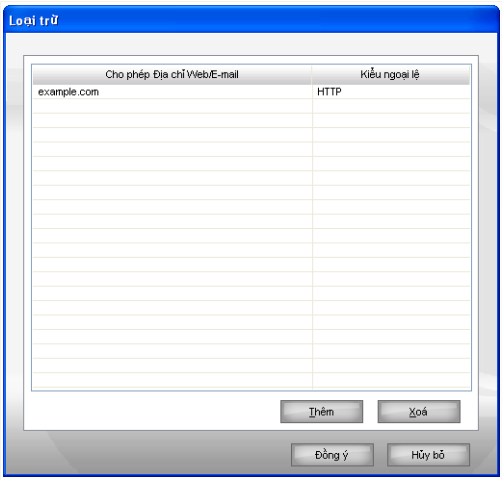
Vào một mô tả ngắn của qui tắc trong trường sửa.

Nhấp vào **Kết thúc**.

8.2.2. Định nghĩa các ngoại lệ

Có trường hợp bạn cần phải định nghĩa ngoại lệ để đặt qui tắc dữ liệu cá nhân. Có các trường hợp bạn cần chỉ rõ các ngoại lệ để cho các quy tắc bảo mật. Hãy lưu ý đến các trường hợp khi bạn thết lập quy tắc bảo mật để ngăn chặn việc gửi số thẻ tín dụng của bạn qua HTTP (web). Bất cứ khi nào số thẻ tín dụng của bạn được gửi lên trang web thông qua tài khoản người dùng, trang web tương ứng sẽ bị ngăn chặn. Nếu bạn muốn, ví dụ như, mua một đôi giầy từ một cửa hàng trực tuyến (bạn đã chắc chắn về mức độ an toàn bảo mật), bạn sẽ phải tạo một quy tắc ngoại lệ tương ứng.

Để mở cửa sổ nơi bạn có thể quản lý các trường hợp ngoại lệ, Nhấn **Ngoại lệ**.



Ngoại trừ

Thêm một ngoại lệ, làm theo các bước sau:

1. Nhấp vào **Thêm** để thêm một mục mới trong bảng.
2. Ấn đúp chuột vào **Các địa chỉ được cho phép** và chỉ định địa chỉ trang web hoặc địa chỉ email mà bạn muốn làm ngoại lệ.
3. Ấn đúp chuột vào **Chọn kiểu** và lựa chọn từ trình đơn tùy chọn tương ứng với các kiểu địa chỉ đã nêu trước đó.
   - Nếu như bạn đã chỉ định 1 địa chỉ web, chọn **HTTP**.
   - Nếu như bạn chọn một địa chỉ email, chọn **SMTP**.

Để xóa một ngoại lệ khỏi danh sách, chọn nó và ấn **Xóa**.

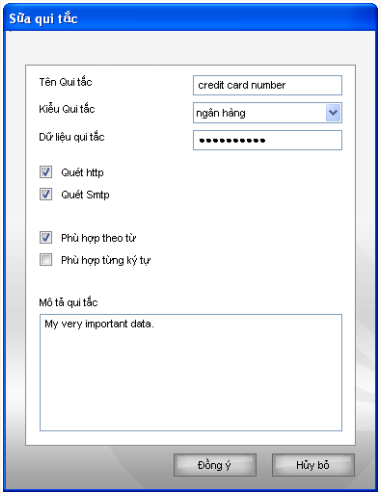
Nhấn**Đồng ý** để lưu sự thay đổi.

8.2.3. Quản lý các quy tắc

Bạn có thể thấy danh sách qui tắc trong bảng.

Để xoá một qui tắc, hãy nhấp vào nút **Xoá**. Nếu bạn chỉ muốn tạm thời dừng qui tắc mà không xoá, hãy bỏ tích phần này.

Để sửa một qui tắc hãy chọn và bấm vào nút **Sửa** hoặc nhấp kép. Cửa sổ sau đây sẽ hiện lên:



Sửa Qui tắc

Tại đây bạn có thể thay đổi tên, mô tả và thông số của qui tắc (loại, dữ liệu và giao dịch). Nhấp chuột vào nút **OK** để lưu lại.

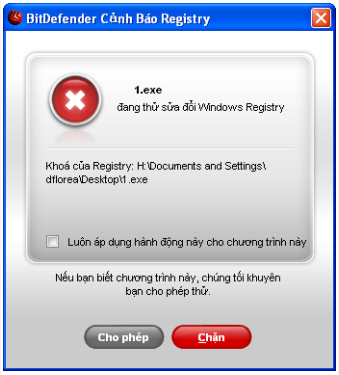
Nhấp **OK**để lưu lại các thay đổi và đóng cửa sổ lại.

8.3. Cài đặt cấp cao - Kiểm soát Registry

Một phần hết sức quan trọng của hệ thống Windows được gọi là **Registry**. Đó là việc Windows giữ lấy cài đặt, chương trình cài đặt, thông tin người dùng, v.v...

Registry đồng thời được dùng để định nghĩa chương trình nào có thể khởi động tự động cùng với Windows. Virus thường dùng nơi này để tự động khởi động cùng với máy tính của bạn.

Kiểm soát Registry để ý đến Windows Registry - đây cũng việc hữu ích cho việc phát hiện Trojan horses. Nó luôn cảnh báo bạn khi có một chương trình muốn khởi động tại Windows start-up.



Cảnh báo Registry

Bạn có thể chặn những thay đổi bằng cách nhấn **No** hoặc bạn có thể cho phép khi nhấn **Yes**.

Nếu bạn muốn BitDefender nhớ câu trả lời của bạn, bạn cần phải tích vào: **Nhớ hành động cho chương trình này**. Trong trường hợp này, một quy tắc sẽ được tạo và hành động giống thế sẽ được áp dụng bất cứ khi nào chương trình cố thay đổi một bản ghi của registry để thực thi khi Windows khởi động.

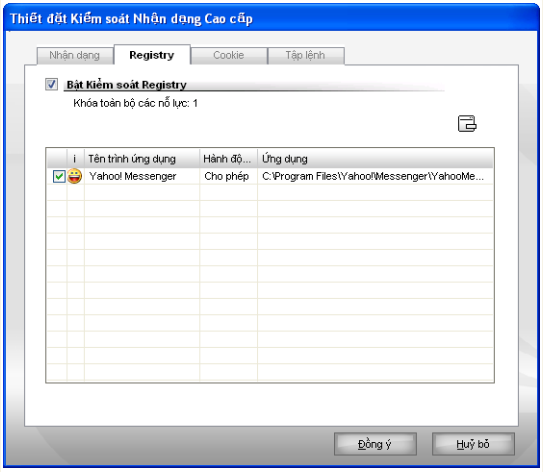
Ghi chú

BitDefender sẽ thường xuyên cảnh báo khi bạn cài đặt chương trình mới mà phải chạy trong phần startup khi khởi động lại máy tính. Đa số các trường hợp, những chương trình được phép có thể tin tưởng được.

Mọi qui tắc đã được ghi nhớ đều có thể truy cấp được qua vùng **Registry** để điều chỉnh như fine-tuning. Để truy xuất vào phần này, mở cửa sổ **Thiết lập kiểm soát riêng tư nâng cao** và chọn thẻ **Registry**.

Ghi chú

Để mở cửa sổ **Thiết lập kiểm soát nhận dạng nâng cao** , nhấn **Trạng thái kiểm>soát cá nhân** trong bảng điều khiển thiết lập và ấn **Thiết lập nâng cao**.



Kiểm soát Registry

Bạn có thể thấy danh sách qui tắc được thiết lập trong bảng.

Để xóa một qui tắc hãy chọn và bấm vào nút **Xóa**. Để tắt hoàn toàn một quy tắt mà không xóa nó, hãy gỡ bỏ dấu trong hộp chọn tương ứng.

Để thay đổi hành động của một quy tắc, nhấp đúp vào trường hành động và chọn phương án phù hợp từ thực đơn.

Nhấp **OK**để đóng cửa sổ lại.

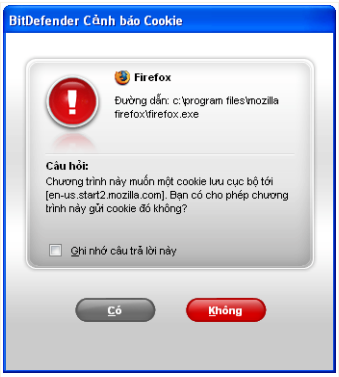
8.4. Cài đặt cấp cao - Kiểm soát cookie

Cookies rất chung cho cho các ứng dụng Internet. Nó là 1 file nhỏ trong máy tính. Websites tạo những cookies này để nhớ những thông tin về bạn.

Cookie thường dùng để giúp đỡ bạn khi sử dụng. Ví dụ như giúp bạn nhớ những tên người dùng và mật khẩu và những thông tin khác, để bạn khỏi phải gõ mỗi khi quay lại web site đó.

Nhưng cookie cũng có thể được dùng để xâm phạm vào vùng riêng tư của bạn, bằng cách theo dõi những khuôn mẫu vào web của bạn.

Đây là nơi mà **Kiểm soát Cookie** có thể giúp. Khi kích hoạt, **Kiểm soát Cookie** sẽ hỏi bạn cho phép những website được thay đổi cookie hay không:



Cảnh báo Cookie

Bạn có thể xem tên của ứng dụng mà nó muốn gửi file cookie.

Tích vào lựa chọn **Nhớ trả lời này** và click **Yes** hoặc **No** và qui tắc sẽ được tạo, áp dụng và lên danh sách trong bảng qui tắc. Bạn sẽ không bị nhắc lại lần sau nữa nếu như vào lại site đó.

Việc này giúp bạn chọn website nào bạn có thể tin tưởng được và website nào không.

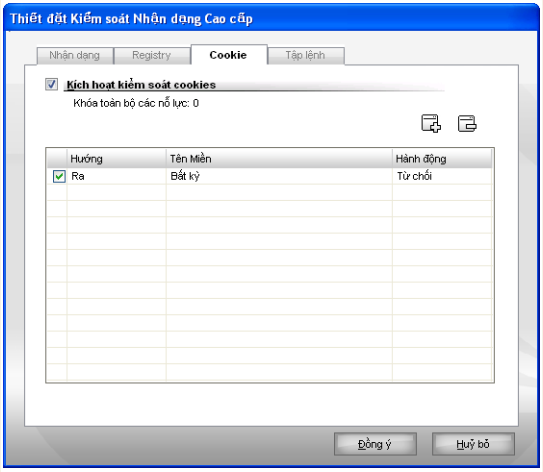
Ghi chú

Vì hiện nay người ta dùng vô số cookie, nên dùng **Kiểm soát Cookie** có thể gây ra phiền muộn. Lúc đầu, nó sẽ rất nhiều câu hỏi bạn về 1 web site muốn ghi cookie vào máy tính của bạn. Khi bạn thêm những qui tắc vào thì nó lập thành một danh sách quy tắc, sau đó thì việc truy cập sẽ nhẹ nhàng như trước.

Mỗi qui tắc đã được ghi nhớ có thể được cho phép vào phần **Cookie** tiếp tục giống như việc điều chỉnh fine-tuning. Để truy cập vào mục này, mở cửa sổ **Advanced Antispyware Settings (Thiết lập Antispyware nâng cao)** và kích chuột vào tab **Cookie**.

Ghi chú

Để mở cửa sổ **Thiết lập kiểm soát nhận dạng nâng cao** , nhấn **Trạng thái kiểm>soát cá nhân** trong bảng điều khiển thiết lập và ấn **Thiết lập nâng cao**.



Kiểm soát Cookie.

Bạn có thể thấy danh sách qui tắc được thiết lập trong bảng.

Quan trọng
Qui tắc mà được lưu lại theo thứ tự ưu tiên từ trên xuống. Qui tắc Drag&drop theo thứ tự để thay đổi ưu tiên.

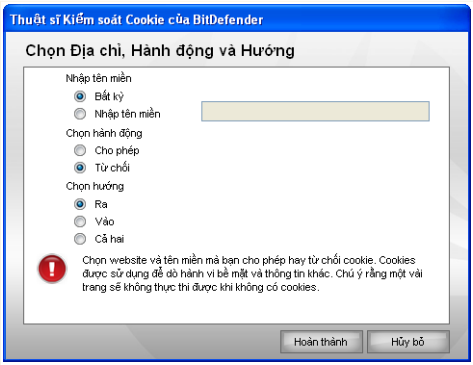
Để xoá một qui tắc, hãy chọn nó và nhấp vào nút **Delete**. Để thay đổi thông số của qui tắc hãy nhấn đúp trường của nó và sửa. Để tạm thời ngừng qui tắc mà không xoá thì chỉ cần bỏ tích.

Qui tắc có thể được vào tự động (qua cửa sổ cảnh báo) hoặc thủ công (click nút **Thêm** và chọn thông số cho nguyên tắc). Thuật sĩ cài đặt sẽ hiện lên.

8.4.1. Thuật sĩ (Wizard) cài đặt

Thuật sĩ cài đặt bao gồm 1 bước.

Bước 1/1 - Chọn Địa chỉ, Hanh động và Phương hướng



Chọn Địa chỉ, Hanh động và Phương hướng

Bạn có thể cài thông số:

- **Tên Miền** - gõ tên miền để áp dụng vào qui tắc.
- **Hành động** - chọn hành động cho qui tắc.

Hành động	Miêu tả
Cho phép	Những Cookie trong miền sẽ được áp dụng.
Chặn	Những Cookie trong miền sẽ không được áp dụng.

- **Hướng** - chọn hướng giao dịch.

Gõ	Miêu tả
Lối ra	Qui tắc này chỉ được áp dụng cho những cookie được gửi ngầm ra ngoài website được nối vào.
Lối vào	Qui tắc chỉ áp dụng cho cookie nhận được từ các website được kết nối.
Cả hai	Qui tắc áp dụng cho cả hai hướng.

Nhấp vào **Kết thúc**.

Ghi chú
Bạn có thể chấp nhận cookie nhưng không bao giờ quay lại khi đặt hành động là **Ngăn chặn** và hướng là **Lối ra**.

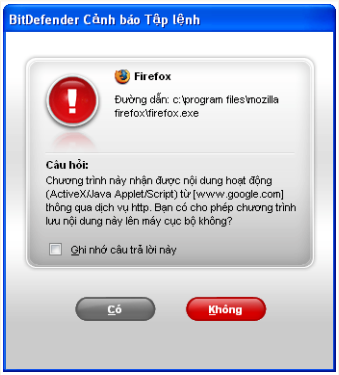
Nhấp **OK**để lưu lại các thay đổi và đóng cửa sổ lại.

8.5. Cài đặt cấp cao - Kiểm soát script

Scripts và ActiveX controls and Java applets, qua đó nó có thể tạo ra phản hồi web site, nhưng có thể tạo ra những hiệu ứng có hại. Những yếu tố ActiveX, ví dụ, có thể chiếm lĩnh hoàn toàn máy tính của bạn và nó có thể đọc được tất cả những dữ liệu của bạn, xoá thông tin, lấy cắp mật khẩu và có thể xem trộm những tin nhắn online của bạn. Bạn chỉ nên chấp nhận active content từ những website mà bạn thực sự tin tưởng.

BitDefender cho phép bạn chọn để chạy hoặc ngăn chăn những nhân tố đó.

Với **Script Control** bạn có thể nạp danh sách những website có thể tin được hay không thể tin được. BitDefender sẽ hỏi ý kiến bạn khi một website muốn khởi động một script hoặc một active content:



Cảnh báo Script

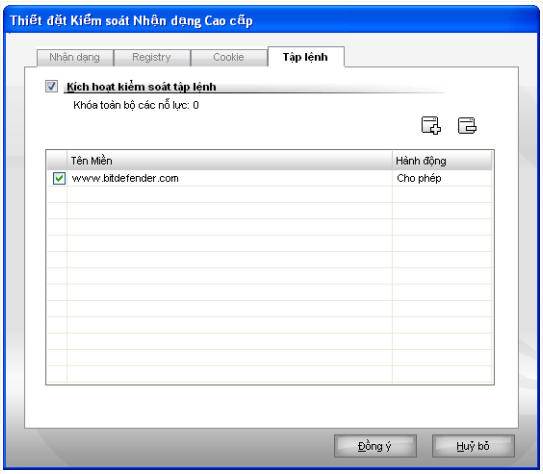
Bạn có thể xem tên nguồn.

Tích vào lựa chọn **Nhớ câu trả lời này** và click **Yes** hoặc **No** và qui tắc được đặt ra, áp dụng và lưu trong bảng qui tắc. Bạn sẽ không bị nhắc lại khi truy cập cùng site kể cả khi nó gửi active content.

Mọi qui tắc đã được ghi nhớ đều có thể truy cấp được qua vùng **Script** để điều chỉnh như fine-tuning. Để truy cập vào mục này, mở cửa sổ **Advanced Identity Control Settings** và kích chuột vào tab **Script**.

Ghi chú

Để mở cửa sổ **Thiết lập kiểm soát nhận dạng nâng cao** , nhấn **Trạng thái kiểm>soát cá nhân** trong bảng điều khiển thiết lập và ấn **Thiết lập nâng cao**.



Kiểm soát Script

Bạn có thể thấy danh sách qui tắc được thiết lập trong bảng.

Quan trọng

Qui tắc mà được lưu lại theo thứ tự ưu tiên từ trên xuống. Qui tắc Drag&drop theo thứ tự để thay đổi ưu tiên.

Để xoá một qui tắc, hãy chọn nó và nhấp vào nút **Delete**. Để thay đổi thông số của qui tắc hãy nhấn đúp trường của nó và sửa. Để tạm thời ngừng qui tắc mà không xoá thì chỉ cần bỏ tích.

Qui tắc có thể được vào tự động (qua cửa sổ cảnh báo) hoặc thủ công (click nút **Thêm** và chọn thông số cho nguyên tắc). Thuật sĩ cài đặt sẽ hiện lên.

8.5.1. Thuật sĩ (Wizard) cài đặt

Thuật sĩ cài đặt bao gồm 1 bước.

Bước 1/1 - Chọn Địa chỉ và Hành động

Chọn Địa chỉ và Hành động

Bạn có thể cài thông số:

- **Tên Miền** - gõ tên miền để áp dụng vào qui tắc.
- **Hành động** - chọn hành động cho qui tắc.

Hành động	Miêu tả
Cho phép	Script trên miền sẽ được thực hiện.
Chặn	Script trên miền sẽ không được thực hiện.

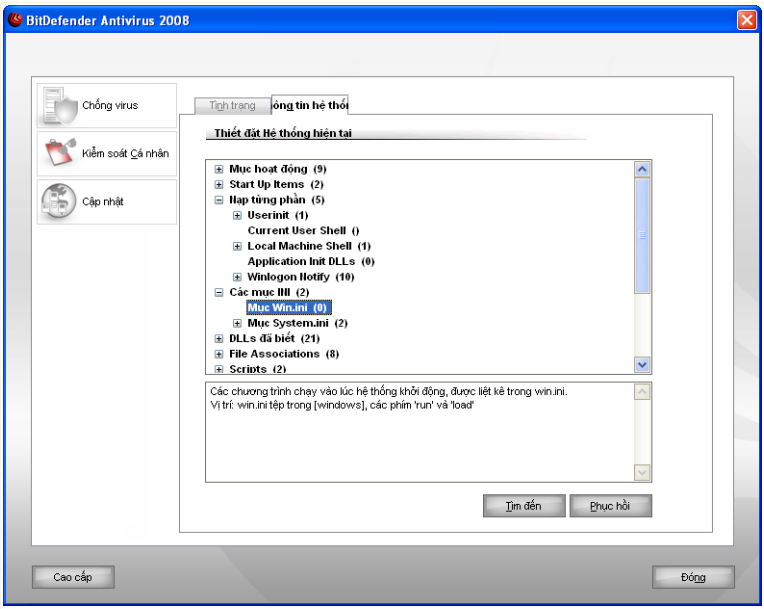
Nhấp vào **Kết thúc**.

Nhấp **OK**để lưu lại các thay đổi và đóng cửa sổ lại.

8.6. Thông tin Hệ thống

BitDefender cho phép bạn xem, từ một địa chỉ riêng lẻ, mọi thiết lập hệ thống và các ứng dụng đã đăng ký chạy lúc khởi động. Theo cách này, bạn có thể theo dõi hoạt động của hệ thống và của các ứng dụng đã được cài lên và cũng như nhận dạng nếu như hệ thống có khả năng bị nhiễm virus.

Để có được thông tin về hệ thống, kích chuột vào **Identity Control>System Info** trong mục settings. Cửa sổ kế tiếp hiện ra:



Thông tin Hệ thống

Danh sách chứa tất cả những mục nạp khi khởi động hệ thống kể cả những mục được nạp bởi những ứng dụng khác.

Ba nút có sẵn:

- **Xoá** - xoá nhiệm vụ được chọn. Bạn phải ấn **Đồng ý**để xác nhận lựa chọn.

> ***Ghi chú***
> Nếu bạn không muốn phải bị nhắc lần nữa để khẳng định lựa chọn của bạn trong cùng một phiên chạy, đánh dấu chọn vào mục **Don't ask me again this session (Đừng hỏi tôi lần nữa trong phiên chạy này)**

- **Đi tới** - mở một cửa sổ mới, từ đó mục được chọn bị thay thế (ví dụ **Registry**).

- **Refresh** - mở lại mục **Thông tin hệ thống**.

Ghi chú

Tùy từng mục đích chọn, một hoặc cả 2 nút **Xóa bỏ** hoặc **Tới** có thể không hiện ra.

8.7. Thanh công Antiphishing

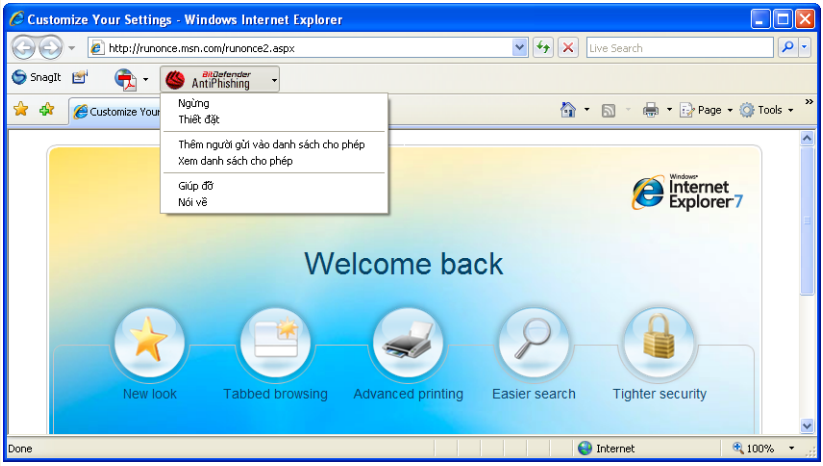
BitDefender bảo vệ bạn khỏi những hành vi lừa đảo khi bạn đang lướt web Nó quét những trang web được truy cập và cảnh báo bạn nếu như có bất kỳ khả năng lừa đảo nào Một Sổ Trắng những website mà không được quét bởi BitDefender có thể được cấu hình.

Bạn có thể quản lý chống lừa đảo và danh sách an toàn một cách dễ dàng và hiệu quả bằng cách sử dụng thanh công cụ BitDefender Antiphishing được tích hợp vào IE.phòng

Thanh công cụ Antiphishing, được thay bởi **Biểu tượng BitDefender**, ở phía trên Internet Explorer. Kích chuột vào đó để mở trình đơn thanh công cụ

Ghi chú

Nếu như bạn không thể nhìn thấy thanh công cụ, mở trình đơn **View**, chỉ chuột đến **Toolbars** và kiểm chuột vào mục **BitDefender Toolbar**.



Thanh công Antiphishing

Các lệnh sau đây có sẵn trên thanh thực đơn:

- **Kích hoạt / Tắt** - kích hoạt / tắt thanh công cụ BitDefender Antiphishing.

> ***Ghi chú***
> Nếu như bạn chọn vô hiệu hóa thanh công cụ chống lừa đảo (anitphishing), bạn sẽ không được bảo vệ trước những nguy cơ lừa đảo.

- **Thiết lập** - mở một cửa sổ tại đây bạn có thể chọn các thiết lập của thanh công cụ antiphishing.

  Có những lựa chọn sau:
  - **Kích hoạt quét Antiphishing**
  - **Hỏi trước khi thêm vào Sổ Trắng** - nhắc bạn trước khi thêm một web vào Sổ Trắng.
- **Thêm vào Sổ Trắng** - thêm trang web hiện tại vào Sổ Trắng.

> ***Ghi chú***
> Thêm một địa chỉ vào Sổ Trắng đồng nghĩa với việc BitDefender sẽ không quét địa chỉ đó nữa. Chúng tôi khuyến cáo bạn chỉ thêm vào danh sách chỉ những địa chỉ mà bạn cực kỳ tin tưởng.

- **Xem Sổ Trắng** - Mở Sổ Trắng.

  Bạn có thể thấy danh sách những websites chưa được kiểm tra bằng công cụ BitDefender antiphishing.

  Nếu bạn muốn xóa một địa chỉ ra khỏi danh sách an toàn để bạn có thể được thông báo về bất cứ nguy cơ lừa đảo nào trên trang đó, hãy kích chuột vào nút **Xóa** ngay kế cạnh nó.

  Bạn có thể thêm những địa chỉ mà bạn hoàn toàn tin tưởng vào danh sách an toàn, và như thế thì những địa chỉ đó sẽ không được quét để chống lừa đảo nữa. Để thêm một trang vào Sổ Trắng, đưa địa chỉ của nó vào trường tương ứng và ấn **Thêm**.
- **Help** - Mở tập tin trợ giúp.
- **About** - mở một cửa sổ nơi bạn có thể xem các thông tin về BitDefender và nơi bạn có thể tìm thấy sự giúp đỡ nếu như có một thứ gì đó không mong đợi xuất hiện.

9. Nâng cấp/cập nhật

Các chương trình nguy hiểm mới được phát hiện và xác định hàng ngày. Đây là lý do tại sao phải luôn cập nhật BitDefender với các chữ ký mới nhất của các chương trình nguy hiêm.

Nếu bạn kết nối với Internet qua broadband hoặc DSL, BitDefender tự làm việc này. Nó sẽ kiểm tra cập nhật từng **giờ** kể từ khi bạn bật máy.

Nếu nó biết có một cập nhật nào đó, tùy thuộc vào lựa chọn của bạn trong phần Lựa chọn cập nhật tự động, bạn sẽ được hỏi nếu muốn hay không muốn cập nhật tự động.

Quá trình nâng cấp đang được thực hiện, có nghĩa là các tệp tin cần nâng cấp được thay thế từng bước một. Bằng cách này, quá trình nâng cấp sẽ không ảnh hưởng đến hoạt động của sản phẩm và cùng lúc mọi cuộc tấn công sẽ bị ngăn chặn.

Việc cập nhật diễn ra theo các cách sau:

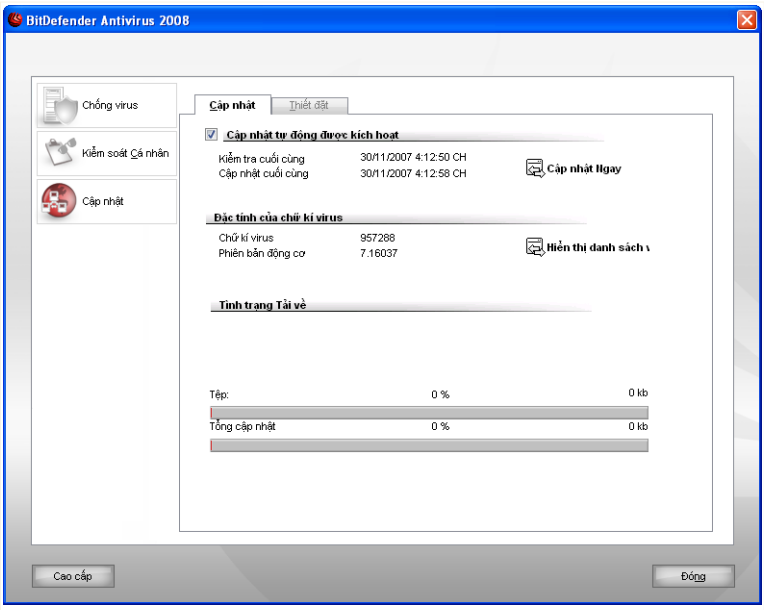
- **Cập nhật cho các đầu diệt virus** - khi các mối đe doạn mới xuất hiện, các tập tin chứa các chữ ký virus phải được cập nhật để đảm bảo việc bảo vệ thường xuyên chống lại chúng. Loại cập nhật này cũng còn được biết đến như **Cập nhật định nghĩa Virus** .
- **Updates for the antispam engines(thực hiện nâng cấp máy chống rác)** - các quy tắc mới sẽ được chèn vào bộ lọc theo kinh nghiệm và bộ lọc theo địa chỉ mạng và các hình ảnh mới sẽ được chèn vào bộ lọc hình ảnh filter. Điều đó tăng cường tính hiệu quả của máy chống rác. Việc nâng cấp, cập nhật cũng được biết đến như là **Antispam Update(nâng cấp chống rác)**.
- **Cập nhật cho các đầu chóng gián điệp** - các chữ ký gián điệp mới sẽ được bổ sung vào cơ sở dữ liệu. Việc cập nhật này cũng được biết đến như **Antispyware Update**.
- **Nâng cấp sản phẩm** - khi một phiên bản sản phẩm mới ra đời, các đặc điểm và các kỹ thuật quét mới sẽ được áp dụng để có hiệu lực với chức năng được nâng cấp của sản phẩm. Loại cập nhật này được biết đến như **Product Update**.

Phần **Cập nhật** của cẩm nang sử dụng này chứa các đề tài sau:

- Cập nhật Tự động
- Cài đặt Cập nhật

9.1. Cập nhật Tự động

Để xem các thông tin cập nhật liên quan và thực hiện tự động cập nhật, ấn **Update>Update** trong bảng điều khiển thiết lập. Cửa sổ kế tiếp hiện ra:



Cập nhật Tự động

Bạn có thể kiểm tra bản cập nhập mới nhất và lần cuối bạn cập nhập cũng như là những thông tin về lần cuối cùng mà bạn cập nhập (nếu như nó thành công hay có lỗi xuất hiện). Thông tin về phiên bản hiện tại và số dấu hiệu được trình bày.

Bạn có thể nhận được chữ ký tin tặc trong BitDefender bằng cách nhấn nút **Hiển thị dah sách virus**. Một file HTML bao gồm những chữ ký virus có thể có đuwocj tạo ngay. Click lần nữa **Hiển thị Danh sách Virus** để xem danh sách. Bạn có thể tìm qua CSDL cho mỗi ứng dụng xấu hoặc click **Danh sách Virus BitDefender** để tra cứu online CSDL chữ ký của BitDefender.

Nếu như bạn mở phần này trong một lần cập nhập, bạn có thể xem được tình trạng đang tải về.

Quan trọng
Để được bảo vệ an toàn chống lại mối đe doạ mới nhất, hãy giữ **Cập nhật Tự động** luôn kích hoạt.

9.1.1. Yêu cầu cho cập nhật

Cập nhật tự động có thể được thực hiện bất cứ lúc nào bạn muốn chỉ cần nhấn nút **Cập nhật ngay**. Cập nhật này cũng được biết như là **Cập nhật theo yêu cầu**.

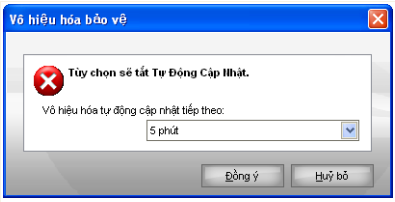
Chức năng **Cập nhật** sẽ kết nối với server cập nhật BitDefender và sẽ kiểm tra xem có cập nhật nào xuất hiện không. Nếu thấy có bất kỳ một cập nhật nào, tuỳ theo cài đặt của bạn trong phần Cài đặt cập nhật thủ công, bạn sẽ được hỏi nếu muốn hay không muốn cập nhật hoặc cập nhật sẽ được tự động thực hiện.

Quan trọng
Có thể cần phải khởi động lại máy tính sau khi bạn cập nhật thành công. Chúng tôi khuyên nên làm việc này càng sớm càng tốt.

Ghi chú
Nếu bạn kết nối với Internet bằng dial-up, bạn nên cập nhật thường xuyên BitDefender theo yêu cầu.

9.1.2. Tắt Cập nhật Tự động

Nếu bạn muốn tắt cập nhật tự động, một cửa sổ tiếp cảnh báo sẽ xuất hiện.



Tắt Cập nhật Tự động

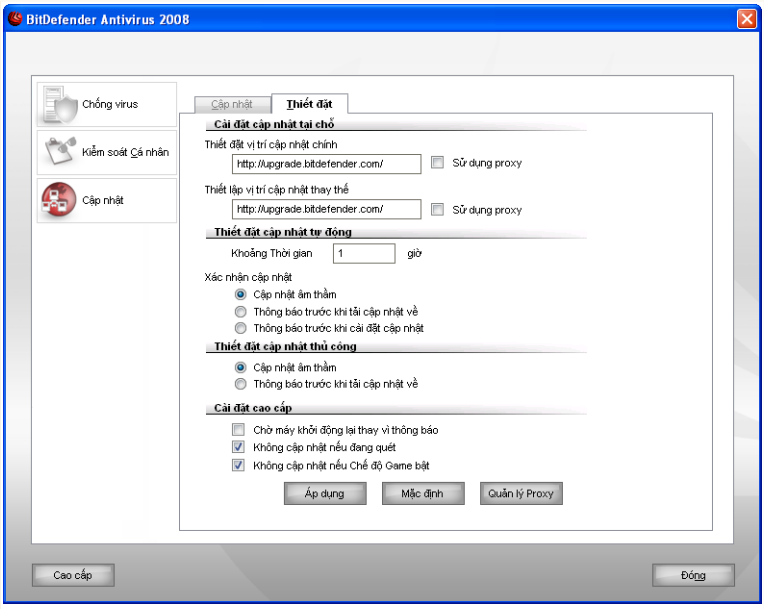
Bạn phải xác nhận lại lựa chọn của bạn bằng cách chọn từ trình đơn bạn muốn vô hiệu hóa chế độ tự cập nhập. Bạn có thể vô hiệu hóa tự động cập nhập trong 5, 15 hay 30 phút, 1 giờ, mãi mãi hoặc cho đến lần khởi động sau.

Cảnh báo
Đây là vấn đề khẩn cấp. Chúng tôi khuyến cáo nên bỏ Cập nhật tự động một giây lát. Nếu BitDefender không cập nhật thường xuyên, nó sẽ không đủ khả năng bảo vệ máy tính cho bạn chống mọi hiểm họa.

9.2. Cài đặt cập nhật

Ccó thể cập nhật từ một máy của mạng LAN, thông qua Internet, trực tiếp hoặc qua proxy server. Theo mặc định, BitDefender sẽ kiểm tra việc cập nhập hàng giờ, qua Internet và cài đặt những cập nhập có sẵn mà không cần nhắc bạn

Để cấu hình về những thiết lập cho việc nâng cấp và quản lý proxy, chọn **Update>Settings** Cửa sổ kế tiếp hiện ra:



Cài đặt cập nhật

Thiết lập cập nhật được nhóm thành 4 danh mục (**Cập nhật nội bộ**, **Tự động nội bộ**, **Cập nhật thủ công** và **Thiết lập nâng cao**). Mỗi danh mục sẽ được mô tả riêng biệt.

9.2.1. Thiết lập vùng Cài đặt Cập nhật

Để xác định vùng cập nhật, sử dụng tùy chọn từ danh mục **Thiết lập vùng cập nhật**.

Ghi chú
Cấu hình những tùy chọn này chỉ nếu khi bạn kết nối tới một mạng cục bộ mà có chứa malware hoặc nếu như bạn kết nối tới một mạng Internet thông một máy chủ proxy.

Để cập nhật nhanh hơn và hiệu quả hơn, bạn có thể cài đặt 2 điểm cập nhật: **Điểm cập nhật sơ cấp** và **Điểm cập nhật thay thế**. Mặc định, các vùng trên là giống nhau: `http://upgrade.bitdefender.com`.

Để thay đổi một trong những địa chỉ cập nhập, đưa ra địa chỉ URL của mirror trong mục **URL** tương ứng với địa chỉ mà bạn muốn thay đổi

Ghi chú
Chúng tôi khuyến cáo bạn thiết lập địa chỉ cập nhập và để địa chỉ cập nhập thay thế không thay đổi, một phương án an toàn trong trường hợp địa chỉ mirror cục bộ không thể truy cập được

Trong trường hợp công ty sử dụng 1 máy chủ proxy để kết nối tới Internet, chọn mục **Dùng proxy** và chọn **Kiểm soát proxy** để thiết lập các tùy chọn proxy

Ghi chú
Để biết thêm thông tin, hãy chuyển đến "*Quản lý proxy*" (p. 109)

9.2.2. Cấu hình cập nhật Tự động

Để cấu hình quá trình BitDefender động cập nhật, sử dụng tùy chọn trong danh mục **Thiết lập tự động cập nhật**.

Bạn có thể đặt thời gian giữa hai lần cập nhật liên tiếp trong trường **Time interval**. Mặc định, khoảng thời gian đó được định là 1 giờ.

Để thiết lập cách thực thi tự động cập nhật, chọn một trong các tùy chọn sau:

- **Cập nhật im lặng** - BitDefender tự động tải và cài đặt cập nhật.
- **Hỏi trước khi tải bản cập nhật** - mỗi khi có bản cập nhật bạn sẽ được hỏi trước khi tải.

Ghi chú
Bạn sẽ được báo trước khi bản cập nhật được tải về ngay cả nếu bạn đã tắt Security Center.

- **Hỏi trước khi cài đặt cập nhật** - sau mỗi khi tải bản cập nhật về bạn sẽ được hỏi trước khi cài.

Ghi chú
Bạn sẽ được nhắc nhở trước khi các bản cập nhật cài đặt thậm chí nếu bạn thoát khỏi Security Center.

9.2.3. Cấu hình cập nhật Thủ công

Để thiết lập cách cập nhật thủ công, chọn một trong các tùy chọn trong danh mục **Thiết lập cập nhật thủ công**:

- **Cập nhật im lặng** - cập nhật thủ công sẽ được thực hiện tự động, không làm người dùng để ý.
- **Hỏi trước khi tải bản cập nhật** - mỗi khi có bản cập nhật bạn sẽ được hỏi trước khi tải.

Ghi chú
Bạn sẽ được báo trước khi bản cập nhật được tải về ngay cả nếu bạn đã tắt Security Center.

9.2.4. Cấu hình thiết lập nâng cao

Để việc nâng cấp BitDefender không làm ảnh hưởng đến công việc của bạn, hãy cấu hình các tùy chọn trong mục **Thiết lập nâng cao**:

- **Chờ khởi động lại, thay vì nhắc** - Nếu như cập nhật đòi hỏi phải khởi động lại máy, sản phẩm có thể giữ cho máy chạy bình thường cho đến khi bạn muốn khởi động lại. Người dùng sẽ không bị BitDefender nhắc khởi động lại sau khi cập nhật và bạn không bị phiền muộn.
- **Không cập nhật khi đang quét** - BitDefender sẽ không cập nhật khi đang quét trên máy. Như vậy việc cập nhật BitDefender sẽ không bị ảnh hưởng đến công việc quét.

Ghi chú
Nếu BitDefender được cập nhật trong khi đang quét, quá trình quét sẽ bị huỷ.

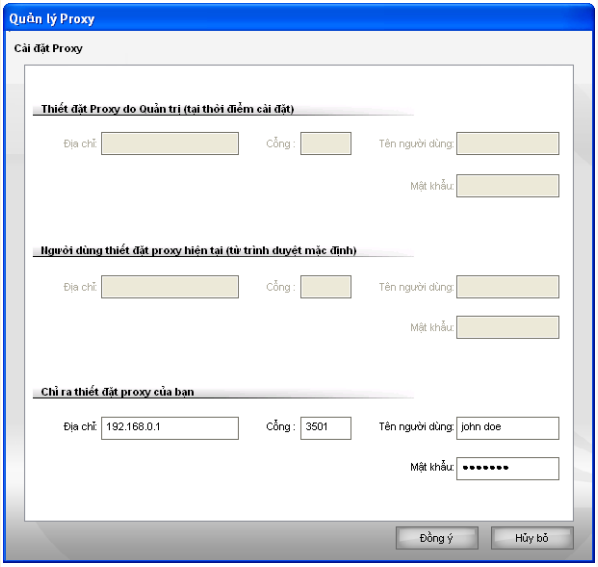
- **Không cập nhật nếu chế độ game đang bật** - BitDefender sẽ không cập nhật nếu chế độ game đang bật. Theo cách này, bạn có thể giảm thiểu được sự ảnh hưởng của sản phẩm thêm hoạt động của hệ thống trong lúc chơi game

9.2.5. Quản lý proxy

Nếu như công ty bạn sử dụng một máy chủ proxy để kết nối tới Internet, bạn phải thiết lập tùy chọn proxy để BitDefender tự động cập nhập. Nếu không, nó sẽ sẽ sử dụng thiết lập proxy của quản trị viên mà được thiết lập khi cài sản phẩm hoặc theo trình duyệt mặc định của người dùng.

Ghi chú
Việc thiết lập proxy chỉ có thể được tinh chỉnh bởi người dùng có quyền quản trị trên máy tính hoặc một nhóm người dùng (biết mật khẩu thiết lập chương trình)

Để quản lý thiết lập proxy, ấn **Quản lý proxy**. Cửa sổ **Quản lý proxy** sẽ xuất hiện.



Quản lý Proxy

Có ba phạm trù của thiết lập proxy:

- **Người quản trị thiết lập proxy (được nhận diện khi cài đặt)** - thiết lập proxy nhận diện tài khoản người quản trị trong quá trình cài đặt và chỉ được cấu hình nếu bạn đăng nhập vào tài khoản đó. Nếu máy chủ proxy yêu cầu tên người dùng và mật khẩu, bạn bắt buộc phải cung cấp trong trường tương ứng.
- **Thiết lập proxy của người dùng hiện tại (từ trình duyệt mặc định)** - Thiết lập proxy của người dùng hiện tại từ trình duyệt mặc định. Nếu bạn đăng nhập vào tài khoản đó. Nếu máy chủ proxy yêu cầu tên người dùng và mật khẩu, bạn bắt buộc phải cung cấp trong trường tương ứng.

> ***Ghi chú***
> Những trình duyệt web được hỗ trợ là Internet Explorer, Mozilla Firefox và Opera. Nếu như bạn sử dụng một trình duyệt khác làm mặc định, BitDefender sẽ không thể lấy được thiết lập proxy của người dùng hiện tại.

- **Thiết lập proxy cá nhân** - Bạn có thể cấu hình proxy nếu bạn đăng nhập với tài khoản người quản trị.

Các thiết lập sau cần được chọn:

- **Địa chỉ** - gõ IP của máy chủ proxy.
- **Cổng** - Gõ cổng mà BitDefender dùng để nối với proxy server.
- **Người dùng** - hãy vào tên người sử dụng mà proxy nhận biết được.
- **Mật khẩu** - hãy vào mật khẩu đúng của người dùng.

Khi cố truy cập đến internet, từng gói thiết lập proxy sẽ được thử lần lượt, cho đến khi BitDefender có thể kết nối được.

Đầu tiên, xác định các thiết lập proxy sẽ được sử dụng để kết nối Internet. Nếu nó không hoạt động, các thiết lập proxy sẽ thử các thiết lập proxy khi cài đặt. Cuối cùng, nếu các trường hợp trên không hoạt động, thì việc thiết lập proxy sẽ lấy từ trình duyệt mặc định của người dùng để kết nối Internet.

Nhấp **OK**để lưu lại các thay đổi và đóng cửa sổ lại.

Nhấp **Áp dụng** để lưu các thay đổi hoặc nhấp vào **Mặc định** để nạp được phần cài đặt mặc định.

Đĩa CD Hồi phục BitDfender

10. Tổng quan

BitDefender Antivirus 2008 đi cùng với một đĩa CD có thể khởi động được (Đĩa CD cứu giúp được dưaj trên LinuxDefender) có khả năng quét và tẩy rửa tất cả các ổ đĩa cứng trước khi bạn khởi động hệ thống.

Bạn cần sử dụng đĩa CD cứu giúp BitDefender bất cứ khi nào hệ thống hoạt động của bạn làm việc không tốt vì bị nhiễm virus. Điều này thường xảy ra khi bạn không sử dụng sản phẩm chống virus.

Việc cập nhật các chữ ký virus được thực hiện tự động mà không cần sự can thiệp của người sử dụng mỗi khi bạn khởi động đĩa CD cứu giúp BitDefender.

LinuxDefender là một loại Knoppix do BitDefender điều khiển, nó hợp nhất sản phẩm mới nhất của BitDefender dành cho giải pháp an ninh Linux với đĩa CD động GNU/Linux Knoppix, cho phép bảo vệ nhanh chống thư rác và virus (SMTP) và chống virus trên màn hình- có khả năng quét và tẩy rửa các ổ cứng hiện hành (Kể cả các phần NTFS của Windows).Tại cùng mộ thời điểm, LinuxDefender có thể được sử dụng để khôi phục các dữ liệu có giá trị của bạn khi bạn không thể khởi động Windows.

10.1. Các yêu cầu của Hệ thống

Trước khi khởi động LinuxDefender, việc đầu tiên bạn phải xác minh xem liệu hệ thống của bạn có đáp ứng được các yêu cầu sau đây hay không.

Loại bộ xử lý

x86 compatible, tối thiểu 166 MHz, nhưng đừng nên trông đợi vào một sự hoạt động hoàn hảo trong trường hợp này. Một bộ xử lý thế hệ i686 generation, 800MHz sẽ là một sự lựa chọn tốt hơn.

Bộ nhớ

Bộ nhớ RAM tối thiểu là 512 MB (khuyến cáo nên sử dụng 1 GB)

CD-ROM

LinuxDefender vận hành từ một CD-ROM, vì vậy, đòi hỏi phải có một CD-ROM và một BIOS có khả năng khởi động từ đó.

Nối mạng Internet

Mặc dù LinuxDefender sẽ vận hành mà không cần phải nối mạng nhưng các thủ tục nâng cấp vẫn sẽ yêu cầu một kết nối HTTP đang hoạt động thậm chí là qua một proxy server. Chính vì vậy, để việc bảo vệ được cập nhật hàng ngày, việc nối mạng Internet là BẮT BUỘC.

Độ phân giải Đồ hoạ
SVGA chuẩn - card đồ họa tương thích.

10.2. Phần mềm được đưa vào

CD cứu giúp của BitDefender bao gồm các gói phần mềm như sau.

Xedit
Đây là một trình chỉnh sửa text

Vim
Đây là một chương trình xử lý tệp tin văn bản mạnh, bao gồm đánh dấu cú pháp, GUI và nhiều tính năng khác. Để biết thêm thông tin, hãy chuyển đến địa chỉ Trang chủ Vim.

Xcalc
Đây là một máy tính.

RoxFiler
RoxFiler là một chương trình quản lý tệp tin ảnh nhanh và mạnh.

ể biết thêm thông tin, hãy chuyển đến địa chỉ Trang chủ RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) là chương trình quản lý tệp tin.

để có thêm thông tin, hãy đi theo đường link MC homepage.

Pstree
Pstree hiển thị những chương tình đang chạy

Top
Top displays Linux tasks.

Xkill
Xkill tắt máy trạm bằng chính tài nguyên X của nó

Ảnh phân vùng
Ảnh phân vùng giúp bạn lưu các phân vùng theo các tệp tin định dạng EXT2,Reiserfs, NTFS, HPFS, FAT16 và FAT32 vào các tệp tin ảnh. Chương trình này rất hữu dụng đối với chức năng sao lưu.

Để có thêm thông tin, hãy truy cập Partimage homepage.

GtkRecover
GtkRecover là một phiên bản GTK của chương trình phục hồi. Nó giúp bạn phục hồi một tập tin

Để có thêm thông tin, hãy truy cập GtkRecover homepage.

ChkRootKit

ChkRootKit là công cụ giúp bạn quét máy tính tìm những rootkits

Để có thêm thông tin, hãy truy cập ChkRootKit homepage.

Thiết bị quét mạng Nessus

Nessus là một máy quét bảo mật từ xa cho Linux, Solaris, FreeBSD, và Mac OS X.

Để có thêm thông tin, hãy truy cập Nessus homepage.

Iptraf

Iptraf là một phần mềm theo dõi mạng IP

Để có thêm thông tin, hãy truy cập Iptraf homepage.

Iftop

Iptop hiển thị băng thông sử dụng trên một giao diện,

Để có thêm thông tin, hãy truy cập Iftop homepage.

MTR

MTR là một tiện ích chẩn đoán mạng

Để có thêm thông tin, hãy truy cập MTR homepage.

PPPStatus

PPPStatus hiển thị trạng thái về lưu lượng TCP/IP vào và ra.

Để có thêm thông tin, hãy truy cập PPPStatus homepage.

Wavemon

Wavemon là một ứng dụng theo dõi các thiết bị mạng không dây

Để có thêm thông tin, hãy truy cập Wavemon homepage.

USBView

USBView hiển thị thông tin về thiết bị kết nối đến bus USB.

Để biết thêm thông tin, vui lòng tham khảo ở Trang chủ.

Pppconfig

Pppconfig giúp tự động thiết lập một kết nối quay số ppp.

DSL/PPPoe

DSL/PPPoe cấu hình cho một kết nối PPPoE (ADSL)

I810rotate

I810rotate liên kết đầu ra video với phần cứng i810 sử dụng i810switch(1).

Để có thêm thông tin I810rotate homepage.

Mutt

Mutt là một ứng dụng mail MIME bằng chữ (text-based) mạnh mẽ.

Để có thêm thông tin, hãy truy cập Mutt homepage.

Mozilla Firefox

Mozilla Firefox là một trình duyệt web nổi tiếng.

Để có thêm thông tin, hãy truy cập Mozilla Firefox homepage.

Elinks

Elinks là một trình duyệt web ở chế độ văn bản (text mode)

Để biết thêm thông tin, vui lòng tham khảo ở Trang chủ Elinks.

11. Đĩa CD Hồi phục BitDfender

Chương này chứa các thông tin làm sao để bắt đầu và ngưng LinuxDefender, quét máy tính bạn tìm malware cũng như lưu dữ liệu từ một máy PC Windows đến một thiết bị di động. Tuy nhiên, bằng cách sử dụng ứng dụng mà đi cùng với CD bạn có thể làm nhiều việc hơn là những gì trong bản hướng dẫn này

11.1. Đĩa CD Hồi phục BitDfender

Để khởi động đĩa CD, cài đặt BIOS cho máy tính của bạn để khởi động được đĩa CD, đặt đĩa CD vào ổ đĩa rồi khởi động lại máy tính. Cần chắc chắn rằng máy tính của bạn có thể khởi động được từ đĩa CD.

Chờ cho đến khi màn hình tiếp theo xuất hiện và theo các chỉ dẫn trên màn hình để khởi động LinuxDefender.

Khởi động màn hình Splash

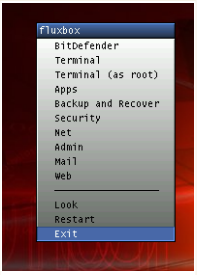
Việc cập nhật các chữ ký virus được thực hiện tự động khi bạn khởi động.

Khi quá trình khởi động kết thúc, bạn sẽ nhìn thấy màn hình nền tiếp theo. Bây giờ bạn có thể sử dụng LinuxDefender.

Màn hình nền

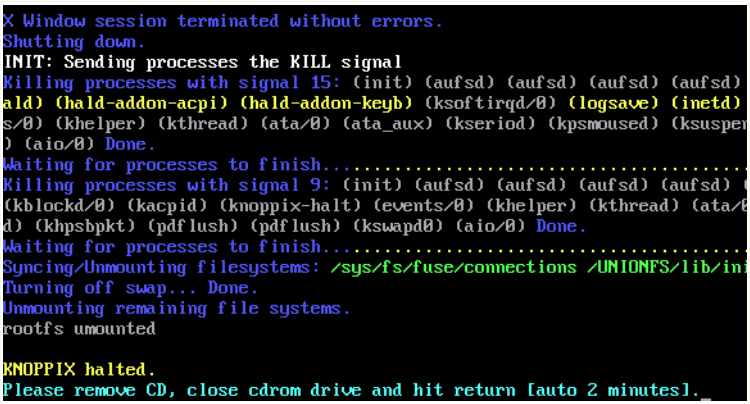
11.2. Đĩa CD Hồi phục BitDfender

Bạn có thể tắt máy tính của mình một cách an toàn bằng cách chọn **Thoát** từ thực đơn LinuxDefender (nhấp chuột phải để mở ra) hoặc bằng cách phát lệnh **halt** trong một thiết bị cuối.



Chọn "EXIT"

Khi LinuxDefender đã đóng thành công tất cả các chương trình, nó sẽ hiển thị một màn hình giống như hình ảnh sau. Bạn có thể lấy đĩa CD ra để khởi động từ đĩa cứng của bạn. Bây giờ bạn có thể tắt máy tính hoặc khởi động lại mà không có vấn đề gì.



Hãy chờ thông điệp này khi tắt máy tính

11.3. Làm cách nào để quét virus?

Một wizard (thuật sĩ) sẽ xuất hiện khi quá trình khởi động kết thúc và cho phép bạn quét toàn bộ máy tính của bạn. Bạn chỉ phải kích chuột vào nút **Start**.

Ghi chú
Nếu như độ phân giải màn hình chưa cao đủ, bạn sẽ được yêu cầu để quét ở chế độ văn bản (text-mode).

Làm theo qui trình 3 bước có hướng dẫn để hoàn thành quá trình quét

1. Bạn có thể xem thấy tình trạng quét và các thống kê (tốc độ quét, thời gian đã quét, số các đối tượng được quét/bị nhiễm/nghi ngờ...).

   Ghi chú
   Quá trình quét có thể mất một lhoảng thời gian, tuỳ thuộc vào độ phức tạp của lần quét.

2. Bạn có thể xem một số ảnh hưởng đến máy tính của bạn.

   Những vấn đề được hiển thị theo nhóm Ấn vào hộp "+" để mở một nhóm hoặc hộp có "-" để đóng một nhóm.

Bạn có thể chọn một hành động toàn diện cho mỗi nhóm vấn đề hoặc bạn cũng có thể tách riêng từng hành động cho mỗi vấn đề.

3. Bạn có thể xem bảng tổng hợp kết quả.

Nếu như bạn muốn quét một thư mục, hãy làm theo:

Duyệt qua các thư mục của bạn, nhấp chuột phải vào một tập tin hoặc một thư mục và chọn **Gửi đến** . Sau đó chọn **Máy quét BitDefender** .

Hoặc bạn có thể phát lệnh tiếp theo như lệnh gốc, từ một terminal. **Máy quét virus BitDefender** sẽ khởi động với các tập tin hoặc các thư mục như các vị trí mặc định để quét.

```
# bdscan /path/to/scan/
```

11.4. Làm thế nào để cập nhật BitDefender qua proxy?

Nếu có một server proxy giữa máy của bạn và internet, cần phải cấu hình thêm để có thể cập nhật được.

Để cập nhật BitDefender qua proxy phải tiến hành những bước sau:

1. Nhấn chuột phải trên Desktop. Menu của CD BitDefender Rescue CD sẽ hiện lên.
2. Chọn **Đầu cuối (như root)**.
3. Gõ lệnh: **cd /ramdisk/BitDefender-scanner/etc**.
4. Gõ lệnh: **mcedit bdscan.conf** để sửa file bằng cách dùng GNU Midnight Commander (mc).
5. Bỏ comment dòng dưới đây: `#HttpProxy =` (chỉ cần xóa `#` dấu) và domain chỉ định, tên, mật khẩu và server port của proxy server. Ví dụ, phải hiện thị giống như sau:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Nhấn **F2** để lưu file này, khẳng định lưu, sau đó nhấn **F10** để đóng.
7. Gõ lệnh: **bdscan update**.

11.5. Tôi lưu dữ liệu của tôi như thế nào ?

Hãy giả sử rằng bạn không thể khởi động Windows PC của bạn vì một lý do nào đó. Cùng lúc đó, bạn lại rất muốn truy cập một số thông tin quan trọng từ máy tính. Đây chính là lúc LinuxDefender trở nên có ích.

Để lưu dữ liệu bạn từ máy tính bạn đến một thiết bị di động, như là một thẻ nhớ USB, bạn hãy làm theo những bước sau:

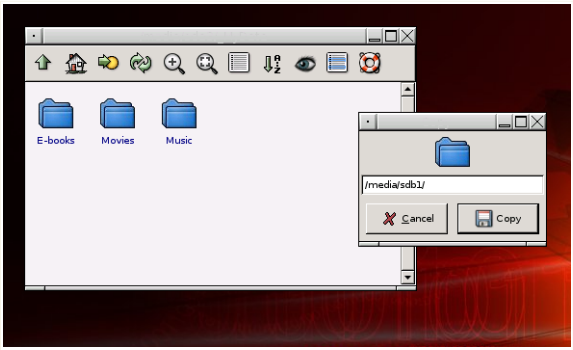
1. Cho LinuxDefender vào ổ CD, thẻ nhớ vào USB sau đó khởi động lại máy
2. Chờ cho đến khi LinuxDefender kết thúc việc khởi động. Cửa sổ sau sẽ xuất hiện.

Màn hình nền

3. Nhấp chuột đôi vào phân vùng mà dữ liệu bạn cần lưu e.g. `[sda3]`).

> ***Ghi chú***
> Khi làm việc với LinuxDefender, bạn sẽ giải quyết với tên phân vùng dạng Linux. Vì thế `[sda1]` sẽ có khả năng tương ứng với `(C:)` phân vùng dạng Windows, `[sda3]` đến `(F:)`, và `[sdb1]` đến thẻ nhớ.

4. Truy cập đến thư mục và mở thư mục mong muốn. Ví dụ, `MyData` nơi mà chứa `Movies`, `Music` và `E-books` thư mục con.
5. Hãy nhấn phải chuột vào thư mục mong muốn và chọn**Sao chép**. Cửa sổ sau sẽ hiện ra.



Lưu trữ dữ liệu

6. Đánh `/media/sdb1/` vào mục tương ứng và chọn **Copy**.

Nhận trợ giúp

12. Hỗ trợ

Như một nhà cung cấp sản phẩm có uy tín, BitDefender luôn cố gắng dành cho khách hàng sự hỗ trợ nhanh, chính xác và ở mức độ cao nhất. Trung tâm Hỗ trợ (mà bạn có thể liên lạc theo địa chỉ dưới đây) luôn cố gắng theo kịp để xử lý các mối đe doạ mới nhất đối với máy tính. Trung tâm là nơi tất cả các câu hỏi của bạn đều được trả lời đúng lúc và kịp thời.

Với BitDefender, việc cống hiến để tiết kiệm thời gian và tiền bạc cho khách hàng bằng cách cung cấp các sản phẩm tiên tiến nhất với giá cả hợp lý nhất luôn là mối ưu tiên hàng đầu. Hơn nữa, chúng tôi tin tưởng rằng việc kinh doanh thành công luôn dựa trên cơ sở giao tiếp tốt và cam kết hỗ trợ khách hàng tốt nhất.

Bạn luôn được hoan nghênh khi yêu cầu trợ giúp tại support@bitdefender.com vào bất cứ lúc nào. Để được trả lời kịp thời, xin bạn hãy đưa vào email của bạn càng nhiều chi tiết càng tốt về BitDefender của bạn, hệ thống của bạn và miêu tả vấn đề bạn gặp phải một cách càng chính xác càng tốt.

12.1. Cơ sở kiến thức của BitDefender

Cơ sở Kiến thức của BitDefender là một kho trên mạng chứa những thông tin về các sản phẩm của BitDefender. Nó lưu trữ dưới dạng rất dễ truy cập như: các báo cáo về kết quả của công tác hỗ trợ kỹ thuật đang tiến hành, các hoạt động sửa chữa lỗi của các đội phát triển và hỗ trợ của BitDefender cùng với các bài báo về ngăn ngừa virus, việc quản lý các giải pháp của BitDefender cùng với giải thích chi tiết và nhiều bài viết khác.

Cơ sở Kiến thức của BitDefender luôn mở cho công chúng truy cập miễn phí. Các thông tin mở rộng mà cơ sở chứa đựng là một phương tiện khác để cung cấp cho khách hàng các kiến thức về kỹ thuật và các vấn đề họ cần hiểu sâu hơn. Tất cả các yêu cầu về thông tin hoặc các báo cáo về sự cố do khách hàng của BitDefender gửi đến cuối cùng cũng sẽ đi vào Cơ sở Kiến thức của BitDefender, như các báo cáo khắc phục sự cố, các văn bản đối phó với những gian lận, hoặc những bản thông tin bổ sung cho các tập tin hỗ trợ sản phẩm.

Cơ sở Kiến thức của BitDefender luôn có mặt bất cứ lúc nào tại http://kb.bitdefender.com.

12.2. Muốn được giúp

12.2.1. Đến dịch vụ web

Bạn có câu hỏi? Những chuyên gia BitDefender có thể giúp bạn 24/7 qua e-mail, chat, live support trên web site... hoàn toàn miễn phí.

Xin hãy theo đường link sau:

Tiếng Anh

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2194/

Tiếng Đức

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2194/

Tiếng Pháp

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2194/

Tiếng Rumani

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2194/

Tiếng Tây Ban Nha

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2194/

12.2.2. Mở ticket hỗ trợ

Nếu bạn muốn mở ticket hỗ trợ và nhận sự trợ giúp qua e-mail, xin hãy theo những link sau:

English: http://www.bitdefender.com/site/Main/contact/1/
German: http://www.bitdefender.de/site/Main/contact/1/
French: http://www.bitdefender.fr/site/Main/contact/1/
Romanian: http://www.bitdefender.ro/site/Main/contact/1/
Spanish: http://www.bitdefender.es/site/Main/contact/1/

12.3. Thông tin để liên lạc

Thông tin hiệu quả là chìa khoá cho sự thành công trong kinh doanh. Trong 10 năm qua, BitDefender đã tạo dựng được một danh tiếng thực sự bằng cách luôn nỗ lực để có thông tin tốt hơn, vượt cả sự mong đợi của các bạn hàng và đối tác. Nếu bạn có bất cứ thắc mắc gì, xin đừng ngần ngại liên lạc với chúng tôi.

12.3.1. Các địa chỉ Web

Sales department: sales@bitdefender.com
support@bitdefender.com.vn
Documentation: documentation@bitdefender.com
support@bitdefender.com.vn
Marketing: marketing@bitdefender.com
Media Relations: pr@bitdefender.com
support@bitdefender.com.vn
Virus Submissions: virus_submission@bitdefender.com
Spam Submissions: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Product web site: http://www.bitdefender.com
Product ftp archives: ftp://ftp.bitdefender.com/pub
Local distributors: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

12.3.2. Các văn phòng chi nhánh

Các văn phòng chhi nhánh của BitDefender sẵn sang đáp ứng bất cứ yêu cầu nào trong các lĩnh vực hoạt động của mình, cả các vấn đề về thương mại lẫn các vấn đề chung. Các địa chỉ liên lạc của từng văn phòng được liệt kê dưới đây.

Vietnam

BitDefender Asia Pacific
5 Fabrica de Glucoza Street, sector 2,
Bucharest, Romania
Phone: 0040 21 233 0780
Fax: 0040 21 233 0763
Email: sales@bitdefender.com
Support: support@bitdefender.com
Website: www.bitdefender.com

Viami Software JSC
Công ty cổ phần phần mềm VIAMI
Trụ sở Hà Nội:
139 Trung Kính - Trung Hạ - Cầu Giấy - Hà Nội, VIETNAM
ĐT: 00 84 4 784 3558
Email sales: sales@viamisoftware.com
Hỗ trợ: support@bitdefender.com.vn
Hỗ trợ trực tuyến: www.viamisoftware.com

Chi nhánh TP HCM:
131 Thoại Ngọc Hầu P.Phú Thạnh Q.Tân Phú - HCM, VIETNAM
ĐT: 00 84 8 973 6855, 973 6856
Email sales: sales@viamisoftware.com
Hỗ trợ: support@bitdefender.com.vn
Hỗ trợ trực tuyến: www.viamisoftware.com

Trung tâm Phân phối:
17 Tân Quư, Phường Tân Quư Quận Tân Phú, TP HCM, VIETNAM
ĐT: 00 84 8 444 9131
Fax: 00 84 8 847 2467
Email sales: sales-sg@viamisoftware.com
Hỗ trợ: support@bitdefender.com.vn
Hỗ trợ trực tuyến: www.viamisoftware.com

Sổ tay thuật ngữ

Công nghệ ActiveX

Công nghệ ActiveX là một khuôn mẫu để viết các chương trình sao cho các chương trình khác và hệ điều hành có thể hiểu được. Công nghệ ActiveX được sử dụng với chương trình duyệt internet của Microsoft để biến các trang web có tính tương tác, các trang web sẽ có hình thái và cách ứng xử giống như các chương trình máy tính, chứ không giống như các trang tĩnh. Với công nghệ ActiveX, người dùng có thể hỏi và trả lời câu hỏi, có thể sử dụng các nút đẩy và tương tác với các trang web theo nhiều cách thức. Điều khiển ActiveX thường được viết bằng ngôn ngữ Visual Basic.

Công nghệ Active X có hiệu quả khi thiếu các quản lý an ninh; các chuyên gia an ninh máy tính không khuyến khích công nghệ Active X trên internet.

Adware

Adware (advertising ware) là các phần mềm thực hiện quảng cáo, thường được kết hợp với các ứng dụng máy chủ mà được cung cấp miễn phí nếu người dùng đồng ý chấp nhận các phần mềm quảng cáo đó. Bởi vì các ứng dụng của phần mềm quảng cáo thường được cài đặt sau khi người dùng đồng ý với cam kết cấp phép nói rõ mục đích của ứng dụng, không cam kết bất kỳ một lỗi nào.

Tuy nhiên, các mục quảng cáo đổ xuống có thể gây khó chịu, và trong một số trường hợp làm yếu đi khả năng thao tác của hệ thống. Thông tin mà những ứng dụng này thu thập được cũng có thể có liên quan tới tính riêng tư đối với người dùng không thực sự hiểu hết các điều khoản của cam kết cấp phép.

Lưu tin

Archive là đĩa, băng, hoặc thư mục có chứa các tập tin đã được lưu cho mục đích dự phòng.

Một tập tin có chứa một hay nhiều tập tin khác dưới dạng nén.

Cửa sau

Một lỗ hổng an ninh được người thiết kế hay người bảo dưỡng để lại một cách có tính toán. Động cơ của những lỗ hổng này thường không to tát, một vài hệ điều hành, có thể lấy ví dụ vậy, được bật ra với những tài khoản ưu tiên nhằm mục đích cho việc sử dụng bởi các nhà kỹ thuật dịch vụ hay bởi các nhà lập trình bảo dưỡng của hãng cung cấp.

Cung khởi động

Cung khởi động nằm ngay đầu các đĩa sẽ nhận dạng cấu trúc của đĩa (độ lớn cung, độ lớn cluster, v.v). Đối với đĩa khởi động, cung khởi động cũng chứa chương trình tải hệ điều hành.

Virus khởi động

Virus khởi động là một loại virus tác động lên cung khởi động của một đĩa cố định hay đĩa mềm. Cố gắng khởi động từ một đĩa bị nhiễm virus sẽ biến virus hoạt động trong bộ nhớ. Mỗi lần bạn khởi động hệ thống từ cung khởi động đó, bạn sẽ có virus hoạt động trong bộ nhớ.

Trình duyệt

Browser, dạng viết ngắn của Web browser, là một ứng dụng phần mềm được sử dụng để định vị và hiện thị các trang Web. Hai trình duyệt thông dụng nhất là Netscape Navigator và Microsoft Internet Explorer. Hai trình duyệt này là hai trình duyệt đồ họa, nghĩa là chúng có thể hiện thị đồ họa tốt như hiện thị văn bản dữ liệu. Thêm vào đó, phần lớn các trình duyệt hiện đại có thể biểu thị các thông tin dạng đa truyền thông, bao gồm cả âm thanh, hình ảnh, dù chúng có đòi hỏi cài thêm vài chi tiết cho một vài định dạng.

Dòng lệnh

Trong giao diện dòng lệnh, người dùng có thể đánh lệnh trong khoảng trống được cấp ngay trên màn hình, sử dụng ngôn ngữ lệnh.

Cookie

Nội trong ngành công nghiệp internet, cookies được mô tả như những tập tin nhỏ chứa các thông tin về các máy tính đơn lẻ. Các thông tin này có thể được các nhà quảng cáo phân tích và sử dụng để tìm hiểu sở thích và khẩu vị của bạn. Với mục đích này, công nghệ cookie vẫn đang được phát triển và chủ định là để đưa quảng cáo đi đúng theo sở thích của bạn. Đó là con dao hai lưỡi đối với nhiều người, bởi vì một mặt, nó có hiệu quả và xác đáng khi bạn chỉ xem quảng cáo về các điều bạn thích. Mặt khác, nó bao gồm cả các thao tác "tìm" và "theo" nơi bạn đến và bạn nhấn chuột vào đâu. Có thể hiểu được điều này, có sự tranh luận về tính riêng tư và nhiều người cảm thấy bị xúc phạm khi biết được rằng họ được phỏng vấn như "một con số SKU" (Bạn biết không, đó là mã vạch nằm phía sau một gói hàng để quét tại bàn tính tiền của một cửa hàng rau quả). Trong khi quan điểm này có thể là quá khích, thì trong một vài trường hợp quan điểm đó là chính xác.

Ổ đĩa

Là một máy đọc dữ liệu từ đĩa và ghi dữ liệu lên đĩa.

Một ổ đĩa cứng đọc và ghi lên đĩa cứng.

Một ổ đĩa mềm truy cập đĩa mềm.

Ổ đĩa có thể là ổ đĩa trong (nằm cố định trong một máy tính) hay ổ đĩa ngoài (được gắn với một hộp riêng biệt nối với máy tính).

Tải

Tải là sao chép dữ liệu (thường cả là một tập tin) từ một nguồn chính tới thiết bị ngoại vi. Thuật ngữ này thường được sử dụng để mô tả một quá trình sao chép tập tin từ một dịch vụ trực tuyến vào máy tính cá nhân của một ai đó. Tải có thể mô tả một quá trình sao chép một tập tin từ máy chủ hệ thống tới máy tính trên mạng.

Thư điện tử

E-mail là một thư điện tử. Một dịch vụ gửi tin nhắn vào máy tính thông qua mạng cục bộ hay mạng toàn cầu.

Các sự kiện

Một hành động hay một sự kiện được nhận biết bởi một chương trình. Các sự kiện có thể là hành động của người dùng, ví như nhấp chuột hoặc nhấn một phím, hay các sự kiện hệ thống, ví như bộ nhớ đã cạn.

Nhận diện nhầm

Nhận diện nhầm xảy ra khi chương trình quét nhận diện một tập tin nào đó là nhiễm virus trong khi tập tin đó là sạch.

Phần mở rộng của một tập tin

Phần của một tập tin đi sau dấu chấm, biểu thị dạng dữ liệu được lưu trữ trong tập tin.

Nhiều hệ điều hành sử dụng phần mở rộng của tập tin, ví như Unix, VMS, và MS-DOS. Phần mở rộng thường là từ một tới ba chữ cái (Nhiều hệ điều hành cũ không cho phép quá 3 chữ cái). Ví dụ có thể bao gồm "c" với ngôn ngữ nguồn của C, "ps" với PostScript, "txt" với chương trình dữ liệu dạng văn bản.

Phương pháp theo kinh nghiệm

Heuristic là một hình thức nhận dạng virus mới dựa trên các quy tắc. Phương pháp quét này không dựa trên bản chất của một loại virus cụ thể. Cái hay của phương pháp nhận dạng heuristic là nó không bị các biến thể mới của một con virus đã tồn tại làm mờ mắt. Tuy nhiên, đôi khi nó thông báo các dòng mã nghi ngờ trong các chương trình bình thường, tạo ra hiện tượng gọi là "nhận diện nhầm".

Giao thức internet

Giao thức internet là một giao thức có thể định hướng trong tập các giao thức TCP/IP mà có trách nhiệm định địa chỉ IP, định đường, và phân mảnh cũng như tái gộp các gói IP.

Phần mềm Applet của Java

Java applet là một chương trình Java được thiết kế để chạy trên các trang web. Để sử dụng applet trên một trang web, bạn phải cụ thể tên cũng như kích cỡ của applet (độ dài, độ rộng tính bằng pixel) mà applet có thể tận dụng. Khi một trang web được truy cập, trình duyệt sẽ tải applet từ máy chủ và chạy applet trên máy tính của người dùng (máy trạm). Applet khác các ứng dụng khác là ở chỗ chúng được khống chế bởi một giao thức an ninh nghiêm ngặt.

Ví dụ, mặc dù các applet chạy trên máy khách, chúng không thể đọc hoặc ghi dữ liệu lên máy trạm. Hơn nữa, applet thường bị hạn chế sao cho chúng chúng chỉ có thể đọc và ghi dữ liệu từ cùng phạm vi mà chúng đang được phục.

Các virus dưới dạng macros

Là một dạng của các virus máy tính được viết dưới dạng macro nhúng trong tài liệu. Nhiều ứng dụng, ví dụ như Microsoft Word và Excel, có ngôn ngữ macro hùng mạnh.

Các ứng dụng này cho phép nhúng macro trong tài liệu, và macro sẽ được kích hoạt tại mỗi thời điểm tài liệu được mở.

Máy trạm có chức năng thư điện tử

Máy trạm có chức năng thư điện tử là một ứng dụng cho phép bạn nhận và gửi thư điện tử.

Bộ nhớ

Bộ nhớ là vùng lưu trữ trong máy tính của bạn. Thuật ngữ memory mô tả kho dữ liệu dưới dạng các con chíp, và từ storage được sử dụng cho các bộ nhớ tồn tại trên băng hay đĩa. Mỗi máy tính có một dung lượng bộ nhớ vật lý nào đó, và thường được nói đến như bộ nhớ chính hay bộ nhớ RAM.

Phương pháp không theo kinh nghiệm

Phương pháp quét này dựa trên bản chất của một loại virus cụ thể nào đó. Cái được của phương pháp Non-heuristic là ở chỗ nó không bị những cái tưởng là virus làm mờ mắt, và không cảnh báo nhầm.

Các chương trình đóng gói

Chương trình đóng gói là một tập tin dưới dạng nén. Nhiều hệ điều hành và nhiều ứng dụng chứa các câu lệnh cho phép bạn đóng gói một tập tin làm sao để tập tin đó tốn ít bộ nhớ hơn. Ví dụ, bạn đang có một tập tin dạng văn bản có chứa 10 ký tự trống liên tiếp. Thông thường, điều đó đòi hỏi phải có 10 bytes bộ nhớ.

Tuy nhiên, một chương trình đóng gói tập tin có thể thay thế các ký tự trống bằng một ký tự trống đặc biệt và tiếp theo là một cơ số các khoảng trống được thay thế. Trong trường hợp này, 10 ký tự có thể chỉ tốn đến 2 bytes. Đó cũng chỉ là một kỹ thuật đóng gói, và còn nhiều kỹ thuật đóng gói hơn thế nữa.

Đường dẫn

Là hướng dẫn đường đi một cách chính xác tới một tập tin trong máy tính. Các hướng dẫn này thường được mô tả như các cách thức của một hệ thống lưu trữ phân cấp từ trên xuống dưới.

Đường dẫn giữa hai điểm, giống như các kênh giao tiếp giữa hai máy tính.

Phishing

Phishing là hành động gửi một thư điện tử tới một người sử dụng nào đó, nói rằng mình là một cá nhân hợp pháp nhằm yêu cầu người sử dụng cung cấp các thông tin cá nhân được dùng để định dạng trộm. Thư điện tử này sẽ chỉ đường cho người dùng tới thăm một trang web nơi họ được đề nghị cập nhật các thông tin cá nhân, ví như mật khẩu và thẻ tín dụng, an ninh xã hội, và các số hiệu tài khoản ngân hàng, những số liệu mà các tổ chức hợp pháp có. Trang web, tuy nhiên, là trang ma, và được dựng lên để ăn cắp thông tin người dùng.

Virus đa sắc

Là một loại virus thay đổi hình thái theo từng tập tin chúng nhiễm. Vì chúng không có các thành phần nhị phân bất biến, nên virus loại đó là rất khó nhận dạng.

Cổng kết nối

Là một giao diện trên máy tính mà bạn có thể cắm thiết bị vào đó. Máy tính cá nhân có nhiều loại cổng. Xét về thiết bị trong, có vài cổng nối ổ cứng, màn hình, và bàn phím. Xét về thiết bị ngoài, máy tính cá nhân có cổng để nối modem, máy in, con chuột, và các thiết bị ngoại vi khác.

Trong mạng TCP/IP và mạng UDP, cổng kết nối là một điểm cuối tới kết nối lô gích. Số hiệu cổng kết nối định ra nó là loại cổng nào. Ví dụ, cổng 80 được sử dụng cho giao thông loại HTTP.

Tập tin báo cáo

Tập tin báo cáo là một tập tin liệt kê các hành động xảy ra. BitDefender có một tập tin báo cáo các đường dẫn, các thư mục, các tập lưu dữ liệu và các tập tin đã quét, bao nhiêu tập tin nhiễm virus và bao nhiêu tập tin đáng ngờ được tìm thấy.

Rootkit

Rootkit là một bộ các công cụ phần mềm cung cấp quyền truy cập mức quản trị tới một hệ thống. Thuật ngữ lần đầu tiên được sử dụng cho hệ điều hành UNIX, và nó nói đến các công cụ biên dịch, cung cấp cho người xâm phạm các quyền

quản trị, cho phép họ che dấu sự có mặt của họ sao cho các quản trị mạng không nhìn thấy.

Vai trò chính của rootkit là làm ẩn các quá trình, các tập tin, các sự truy cập cũng như các thao tác. Các rootkits có thể chặn dữ liệu từ các máy, từ kết nối mạng hay từ cá thiết bị ngoại vi, nếu chúng hợp nhất với các phần mềm tương thích.

Về mặt bản chất, Rootkit là không phá hoại. Ví dụ, hệ thống và thậm chí một vài ứng dụng dấu các tập tin có tính phê phán bằng cách sử dụng rootkit. Tuy nhiên, chúng được sử dụng phần lớn để dấu các phần mềm phá hoại hoặc dấu sự có mặt của một kẻ xâm phạm không hợp pháp vào hệ thống. Khi được kết hợp với các phần mềm phá hoại, rootkits sẽ có sự đe dọa lớn tới tính toàn vẹn và an ninh hệ thống. Chúng có thể điều khiển giao thông, tạo các cửa hậu trong hệ thống, thay đổi tập tin và nhật trình và chống lại sự bị phát hiện.

Script

Một thuật ngữ nữa của tâp tin đa lệnh, script là một danh sách có thể được hoạt động không cần sự tương tác người dùng.

Spam

Là các thư rác hay các dòng nhắn hàng loạt không ý nghĩa. Thông thường spam được biết đến như là các thư điện tử không mong muốn.

Phần mềm gián điệp

Spyware là bất kỳ phần mềm nào mà thu thập thông tin người dùng thông qua kết nối internet mà người dùng không nhận biết được, thường là cho các mục đích quảng cáo. Các ứng dụng Spyware được bó lại dưới dạng các yếu tố ẩn của một phần mềm miễn phí hoặc chương trình phần mềm chia sẻ mà có thể được tải từ internet xuống; tuy nhiên, cần phải lưu ý rằng mục đích chính của các ứng dụng chia sẻ và ứng dụng miễn phí không đi kèm vớispyware. Khi đã được cài đặt, spyware quản lý hành động trên internet và truyền các dữ liệu cơ sở tới một ai đó. Spyware cũng thu thập thông tin về các địa chỉ thư điện tử và thậm chỉ mật khẩu cũng như số thẻ tín dụng.

Sự tương tự của Spyware với Trojan là ở chỗ người sử dụng cài đặt sản phẩm một cách không có ý thức khi họ cài đặt một cái gì đó khác. Kiểu trở thành nạn nhân của spyware một cách phổ biến là tải các sản phẩm đổi tập tin đồng đẳng mà đang có sẵn ngày nay.

Ngoài vấn đề đạo đức và tính riêng tư, spyware còn ăn trộm của người dùng bằng cách sử dụng tài nguyên bộ nhớ máy tính và tiêu tốn băng thông khi nó gửi thông tin về địa chỉ cung cấp spyware thông qua kết nối internet của người dùng. Bởi vì spyware sử dụng bộ nhớ và tài nguyên hệ thống, nên các ứng dụng chạy

trên nền đó có thể dẫn tới việc phá hủy hệ thống hoặc tạo sự mất ổn định của hệ thống chung.

Startup items

Bất kỳ tập tin nào trong thư mục này (Startup items) đều mở khi máy tính khởi động. Ví dụ, một màn hình khởi động, một tập tin âm thanh được chạy khi máy tính khởi động, một lịch nhắc việc, hay các chương trình ứng dụng đều có thể là các mục khởi động. Thông thường, bí danh của tập tin được đặt trong thư mục chứ không phải bản thân tập tin đó.

Khay hệ thống

Được giới thiệu trong Windows 95, khay hệ thống được đặt tại thanh nhiệm vụ (taskbar) trong Windows (thường là nằm phía dưới màn hình, cạnh đồng hồ), nó bao gồm các biểu tượng nhỏ để truy cập một cách dễ dàng hơn các chức năng hệ thống như fax, máy in, modem, âm lượng và nhiều cái khác nữa. Hãy nhấp đôi nút chuột hay nhấp nút chuột phải lên một biểu tượng để xem và truy cập các chi tiết cũng như các điều khiển.

TCP/IP

Nghĩa là giao thức điều khiển truyền tin/giao thức internet. Nó là một bộ các giao thức mạng được sử dụng rộng rãi trên internet. Các giao thức này cung cấp sự giao tiếp thông qua các mạng máy tính có các cấu trúc phần cứng đa dạng và các hệ điều hành khác nhau, được nối với nhau. TCP/IP bao gồm cả các chuẩn mực về cách thức các máy tính giao tiếp với nhau như thế nào cũng như quá trình chuyển đổi dùng cho các mạng nối với nhau và giao thông phân tuyến.

Ngựa Trojan (một loại virus)

Là một chương trình phá hủy tự tô vẽ như mình là một ứng dụng nhân từ. Không giống như virus, ngựa Trojan không tự nhân bản nhưng chúng chính xác là sự phá hủy. Một trong số những loại ngựa Trojan quỷ quyệt nhất là một chương trình nói rằng có thể giệt virus trong máy tính của bạn, nhưng thay vì làm việc đó, nó lại giới thiệu cho các virus mới thâm nhập máy tính của bạn.

Thuật ngữ được lấy trong một câu chuyện của bản trường ca Homer. Trong câu chuyện này, người Hy lạp đã tặng Trojans, kẻ thù của họ, một con ngựa gỗ lớn, bề ngoài như một vật cầu hòa. Sau khi Trojans kéo ngựa vào thành, lính Hy lạp thoát ra khỏi bụng ngựa, mở cổng thành, cho phép đồng đội tiến vào và lấy lại Troy.

Nâng cấp/cập nhật

Update là một phiên bản mới của sản phẩm phần cứng hoặc phần mềm, được tạo ra để thay thế phiên bản cũ của sản phẩm cùng loại. Hơn nữa, một thao tác cài đặt cập nhật là phải kiểm tra để chắc chắn rằng phiên bản cũ đã tồn tại trong máy tính của bạn, nếu không, bạn không thể cài đặt được phiên bản cập nhật.

BitDefender có mô đun cập nhật của riêng mình, nó cho phép bạn kiểm tra một cách thủ công xem có phiên bản mới nào hay không, hoặc cho phép máy tính của bạn cập nhật sản phẩm một cách tự động.

Virus

Virus là một chương trình hoặc một đoạn mã được tải về máy tính của bạn mà bạn không biết và chạy chống lại mong muốn của bạn. Phần lớn các virus có thể tự nhân bản. Tất cả các virus máy tính là do con người tạo nên. Cũng rất dễ tạo ra một virus đơn giản có thể tự nhân bản. Một virus đơn giản cũng rất nguy hiểm bởi vì nó sẽ nhanh chóng dùng chiếm bộ nhớ đang có và biến hệ thống treo. Một dạng virus nguy hiểm hơn là dạng có khả năng tự truyền qua nhiều mạng, vượt qua cả hệ thống an ninh.

Nhận biết virus

Một đoạn nhị phân của virus, được sử dụng bởi các chương trình chống virus để nhận dạng và diệt virus.

Sâu

Sâu là một chương trình truyền bá thông qua mạng. Trong quá trình truyền bá chúng tự nhân đôi. Worm không tự đính kèm các chương trình khác.