bitdefender
ANTIVIRUS v10

10th anniversary

Hướng dẫn

Antivirus

Chống gián điệp

bitdefender
secure your every bit

BitDefender Antivirus v10
Hướng dẫn

BitDefender

Xuất bản 2006.10.18
Version 10

Văn bản Pháp lý


bitdefender
secure your every bit

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 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 SOFTWIN để được sử dụng sản phẩm phần mềm SOFTWIN 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. SOFTWIN 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 chủ yếu 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.

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 SOFTWIN 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 SOFTWIN. 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.

GIỚI HẠN BẢO HÀNH. SOFTWIN 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. SOFTWIN 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. SOFTWIN không đảm bảo rằng BitDefender sẽ không bị gián đoạn hoặc không có lỗi hoặc các lỗi sẽ được hiệu chỉnh ngay lập tức. SOFTWIN không đảm bảo rằng BitDefender sẽ đáp ứng mọi yêu cầu của bạn. SOFTWIN 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, SOFTWIN 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. SOFTWIN 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, SOFTWIN 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 SOFTWIN 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 SOFTWIN 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 SOFTWIN. 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 SOFTWIN 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.

SOFTWIN 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 SOFTWIN cung cấp là bản chiếm ưu thế.

Liên hệ với SOFTWIN, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, or at Tel No: 40-21-2330780 or 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 10** 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 v10**, 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 v10**, 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. xiii)	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`.
option	Tất cả các lựa chọn sản phẩm được in sử dụng các ký tự **mạnh**.
`sample code listing`	Danh sách mã hoá được in với các `ký tự đơn cách`.

Thể hiện	Miêu tả

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

Cuốn sách bao gồm 07 phần, chứa các đề tài chính: Về BitDefender, Lắp đặt Sản phẩm, Miêu tả và các điểm đặc trưng, Bàn Quản lý, Các thực hành tốt nhất, CD Hồi phục BitDefender (Rescue) và Nhận Trợ giúp. Hơn nữa có một cuốn sách chú giải được cung cấp để làm rõ một số thuật ngữ kỹ thuật.

Nói về BitDefender. Giới thiệu tóm tắt về BitDefender. Nó giải thích BitDefender và SOFTWIN là gì.

Cài đặt sản phẩm. 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 v10**. 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.

Miêu tả và các đặc trưng. BitDefender Antivirus v10, các điểm đặc trưng và các module của sản phẩm được giới thiệu với bạn.

Bàn Quản lý. Mô tả các hoạt động quản lý và bảo dưỡng có bản cho BitDefender. Các chương giải thích chi tiết tất cả các phương án của **BitDefender Antivirus v10**, đăng ký sản phẩm như thế nào, quét máy tính của bạn như thế nào và nâng cấp các hạng mục ra sao. Bạn được chỉ dẫn cách cấu hình và sử dụng tất cả các module của BitDefender.

Các thực hành tốt nhất. Làm theo các chỉ dẫn này để khai thác tốt nhất sản phẩm BitDefender.

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.

Nói về BitDefender

1. Tổng quan

BitDefender™ cung cấp các giải pháp an ninh thoả mãn tất cả các yêu cầu bảo vệ của môi trường máy tính hiện nay, đưa ra phương pháp quản lý các mối đe doạ một cách có hiệu quả cho hơn 41 triệu máy tính cá nhân và của các công ty tại hơn 200 quốc gia trên thế giới.

- Các đặc điểm chống virus, tường lửa, chống gián điệp, chống thư rác và kiểm soát trẻ em các máy tính của các công ty và các cá nhân;
- Loạt sản phẩm của BitDefender được thiết kế để hoạt động trong các cấu trúc công nghệ thông tin phức tạp (các máy trạm, file servers, email servers và gateway), trên các nền Windows, Linux và FreeBSD;
- Phân bổ trên toàn thế giới, sản phẩm có sẵn trên 18 ngôn ngữ;
- Dễ sử dụng, với một thuật sĩ (wizard) cài đặt hướng dẫn người sử dụng trong suốt quá trình cài đặt và chỉ đặt một vài câu hỏi;
- Các sản phẩm được cấp chứng chỉ Quốc tế: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, v.v...;
- Chăm sóc khách hàng mọi lúc – Đội chăm sóc khách hàng luôn có mặt mỗi ngày 24 giờ và 7 ngày một tuần;
- Thời gian đáp ứng nhanh với các cuộc tấn công máy tính mới;
- Tỉ lệ phát hiện cao nhất;
- Cập nhật hàng giờ trên Internet những chữ ký của virus mới - Tự động hay quét theo thời gian biểu để bảo vệ chống lại các virus mới nhất.

1.1. Tại sao lại là BitDefender?

Đã được chứng minh. Nhà sản xuất các phần mềm chống virus có phản ứng nhanh nhất. Sự phản ứng nhanh của BitDefender trong trường hợp có dịch virus máy tính đã được khẳng định, bắt đầu với sự bùng nổ gần đây của các loại virus như CodeRed, Nimda and Sircam, cúng như Badtrans.B và các mã nguy hiểm và có khả năng lây lan nhanh khác. BitDefenderlà sản phẩm đầu tiên cung cấp các phương tiện chống lại các mã này và làm cho chúng hoạt động tự do trên Internet cho tất cả các đối tượng nhiễm bệnh. Hiện nay, với sự tiếp tục lây lan của virus Klez - trong nhiều phiên bản khác nhau thì việc bảo vệ chống virus trở nên một nhu cầu cấp thiết đối với bất cứ một hệ thống máy tính nào.

Sáng kiến. Được giải thưởng Sáng tạo của Hội đồng châu Âu và EuroCase. BitDefender được công bố là sản phẩm đoạt giải European IST-Prize, của Cộng đồng

châu Âu và của đại diện 18 viện hàng lâm ở châu Âu. Hiện nay là năm thứ 18, European IST Prize là giải thưởng cho các sản phẩm mang tính đột phá đại điện cho những sáng kiến tốt nhất của châu Âu về công nghệ thông tin.

Toàn diện. Bao quát từng điểm một trong mạng công tác của bạn, bảo đảm an ninh tuyệt đối. Các giải pháp an ninh của BitDefender cho môi trường công ty thoả mãn các yêu cầu bảo vệ của môi trường máy tính hiện nay, nó giúp quản lý tấtc ả các mối hiểm hộ phức tạp, đe doạ mạng, từ một khu vực nội bộ nhỏ cho đến các mạng diện rộng đa máy chủ và đa nền.

Vệ sĩ cuối cùng của bạn. Tiền đồn cuối cùng bảo vệ hệ thống máy tính của bạn khỏi mọi hiểm hoạ. Do việc phát hiện virus dựa trên các phân tích mã không phải lúc nào cũng cho các kết quả tốt, BitDefender đã thực hiện việc bảo vệ dựa trên hành vi, đảm bảo an ninh chống lại các malware mới sinh ra.

Có **các chi phí** các tổ chức muốn tránh và các sản phẩm an ninh nào được thiết kế để phòng tránh:

- Sâu bọ tấn công
- Mất liên lạc do các email bị nhiễm.
- Hư hại E-mail
- Tẩy rửa và khôi phục các hệ thống
- Người sử dụng cuối cùng bị mất năng suất lao động do thiếu các hệ thống
- Việc truy cập của hacker và các đối tượng không được phép tạo ra hư hỏng

Một số hành động đồng thời **các tiến triển và lợi ích** có thể đạt được bằng việc sử dụng bộ sản phẩm an ninh của BitDefender:

- Tăng cường khả năng của mạng bằng cách ngăn chặn sự lây lan của các mã nguy hiểm (Ví dụ như Nimda, Trojan horses, DDoS).
- Bải vệ những người sử dụng từ xa khỏi bị tấn công.
- Giám các chi phí hành chính và triển khai nhanh các khả năng quản lý doanh nghiệp bằng BitDefender.
- Ngăn chặn sự lây lan của các phần mềm xấu qua e-mail, sử dụng chương trình bảo vệ email của BitDefender ngay tại cổng vào của công ty. Ngăn chặn tạm thời hoặc thường xuyên các kết nối ứng dụng trái phép, đắt tiền hoặc có nguy cơ tổn thương cao.

1.2. Về SOFTWIN

Ra đời vào năm 1990, đoạt giải thưởng IST năm 2002, SOFTWIN hiện lại được coi là nhà công nghệ hàng đầu của công nghiệp phần mềm Đông Âu với mức tăng trưởng hàng năm đạt trên 50 % trong năm năm trở lại đây và đạt 70% doanh thu từ xuất khẩu.

Với một đội ngũ gồm hơn 800 nhân viên có chuyên môn cao, và quản lý hơn 10000 dự án từ trước tới nay, SOFTWIN tập trung vào việc cung cấp các giải pháp phần mềm và các dịch vụ phức tạp, giúp các công ty đang phát triển nhanh giải quyết các thách thức cơ bản trong kinh doanh và khai thác các cơ hội kinh doanh mới. Quá trình phát triển của SOFTWIN được cấp chứng chỉ ISO 9001.

Do hoạt động trên hầu hết các thị trường công nghệ thông tin của Hoa Kỳ và Liên minh châu Âu, SOFTWIN phát triển trên 4 interlinked **tuyến kinh doanh s**:

- eContent Solutions
- BitDefender
- Business Information Solutions
- Customer Relationship Management

SOFTWIN có các văn phòng chi nhánh tại **Đức**, **Tây Ban Nha**, **Anh Quốc** và **Hoa Kỳ** .

Cài đặt sản phẩm

2. Cài đặt BitDefender Antivirus v10

Phần **BitDefender Antivirus v10 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 đầu tiên
- Nâng cấp
- Dỡ bỏ, Sửa chữa hoặc thay đổi các chức năng của BitDefender

2.1. Các yêu cầu của Hệ thống

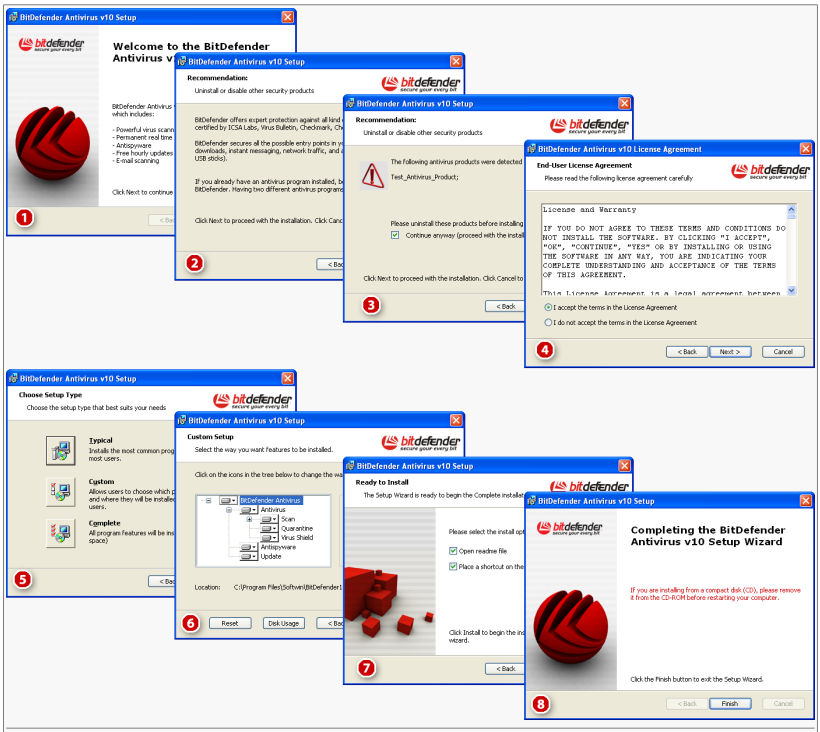
Để đảm bảo cho sản phẩm hoạt động tốt, trước khi lắp đặt cần xác nhận rằng những đòi hỏi về hệ thống sau đây phải được đáp ứng:

- Pentium II 350 MHz hoặc bộ xử lý cao hơn
- Bộ nhớ RAM tối thiểu là 128 MB (khuyến cáo nên sử dụng 256 MB)
- Đĩa cứng phải có dung lượng tối thiểu là 60 MB
- Môi trường hoạt động: Windows 98/NT-SP6/Me/2000/XP IE 5.5 (+)

BitDefender Antivirus v10 có thể tải xuống để đánh giá từ http://www.bitdefender.com website cho công ty SOFTWIN dành cho anh ninh dữ liệu.

2.2. Các bước cài đặt

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



Các bước cài đặt

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 **Tiếp theot** để tiếp tục hoặc nhấp vào **Quay lại** để trở về bước đầu tiên.
3. BitDefender Antivirus 10 sẽ cảnh báo cho bạn nếu có các sản phẩm chống virus khác được cài đặt trong máy tính của bạn.

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.

Nhấp chuột **quay lại** để trở về bước trước đó hoặc **Huỷ bỏl** để thoát khỏi chương trình cài đặt. Nếu bạn muốn tiếp tục, nhấp vào **Tiếp theo**.

Ghi chú
Nếu như BitDefender Antivirus v10 không phát hiện ra các sản phẩm chống virus khác ttrong máy tính của bạn, bạn sẽ bỏ qua bước này.

4. 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.
5. Bạn có thể chọn loại cài đặt bạn muốn: Loại điển hình, loại thông dụng hoặc loại hoàn thiện.

   Điển hình
   Chương trình sẽ được cài đặt với các phương án phổ biến nhất. Đây là phương án được khuyến cáo cho đại đa số người sử dụng.

   Thông dụng
   Bạn có thể lựa chọn các hợp phần mà bạn muốn cài đặt. Chỉ khuyến cáo cho những người sử dụng có trình độ cao.

   Hoàn thiện
   Để lắp đặt hoàn thiện sản phẩm. Tất cả các module của All BitDefender sẽ được cài đặt.

   Nếu bạn chọn **Điển hình** hoặc **Hoàn thiện**, bạn sẽ cỏ qua bước 6.
6. Nếu bạn đã chọn **Tuỳ chọn**, một cửa sổ sẽ xuất hiện chứa tất cả các hợp phần được liệt kê của BitDefender đẻ bạn có thể chọn những phần mà bạn muốn cài đặt.

   Nếu bạn nhấp vào tên của bất cứ hợp phần nào, sẽ có một mô tả vắn tắt (bao gồm cả dung lượng tối thiểu của đĩa cứng) sẽ xuất hiện phía tay phải của bạn. Nếu bạn nhấp vào bất cứ biểu tượng nào của hợp phần, một cửa sổ sẽ xuất hiện khi bạn chọn phương án cài đặt hoặc không cài đặt module được chọn lựa.

   Bạn có thể chọn thư mục nơi bạn muốn cài đặt sản phẩm. Thư mục mặc định là `C:\Program Files\Softwin\BitDefender 10`.

   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 v10. Nhấp vào **Tiếp theo**.
7. 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 v10 trên màn hình nền của bạn vào cuối thời gian cài đặt.

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

Quan trọng
Trong quá trình cài đặt sẽ có một wizard xuất hiện. Cẩm nang (wizard) này giúp bạn đăng ký **BitDefender Antivirus v10**, tạo ra một tài khoản BitDefender và lắp đặt BitDefender để thực hiện các nhiệm vụ an ninh quan trọng.
Hãy hoàn tất quá trình được cẩm nang hướng dẫn để chuyển sang các bước tiếp theo.

8. Nhấp chuột vào **Finish** để hoàn tất việc lắp đặt sản phẩm. Nếu bạn chấp nhận lắp đặt mặc định cho đường dẫn lắp đặt thì một thư mục có tên gọi là `Softwin` được tạo ra trong `Program Files` và nó chứa đựng thư mục phụ `BitDefender 10`.

Ghi chú
Bạn có thể được yêu cầu khởi động lại hệ thống để wizard cài đặt có thể hoàn tất quá trình lắp đặt.

2.3. Wizard cài đặt đầu tiên

Trong quá trình cài đặt, một wizard sẽ xuất hiện. Wizard này giúp bạn đăng ký **BitDefender Antivirus v10**, tạo ra một tài khoản BitDefender và giao cho BitDefender thực hiện các nhiệm vụ an ninh quan trọng.

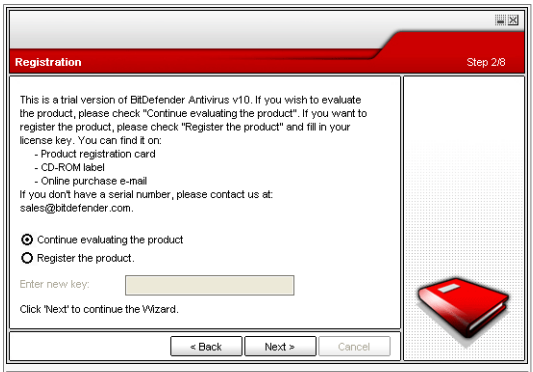
Không bắt buộc phải kết thúc wizard này song chúng tôi khuyến cáo bạn nên làm như vậy để tiết kiệm thời gian và đảm bảo cho hệ thống của bạn an toàn thậm chí là trước khi BitDefender Antivirus v10 được cài đặt.

2.3.1. Bước 1/8 - Thuật sĩ cài đặt BitDefender lần đầu

Cửa sổ chào đón

Nhấp chuột vào **Next**.

2.3.2. Bước 2/8 - Đăng ký BitDefender Antivirus v10



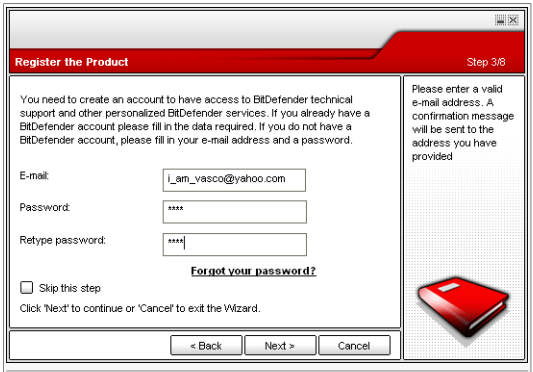
Đăng ký

Chọn **Đăng ký sản phẩm**để đăng ký **BitDefender Antivirus v10**. 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**.

2.3.3. Bước 3/8 - 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.

Đánh địa chỉ email đang còn hiệu lực vào **E-mail** field. Nhớ mật mã và đánh 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 mã phải có ít nhất bốn ký tự.

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.

Quan trọng
Xin hãy kích hoạt địa chỉ email trước khi chuyển sang các bước tiếp theo.

Nếu bạn không muốn tạo ra một tài khoản BitDefender, bạn chỉ cần chọn **Bỏ qua bước này**. Bạn cũng sẽ bỏ qua bước tiếp theo của cẩm nang hướng dẫn (wizard).

Click **Next** to continue or **Cancel** to exit the wizard.

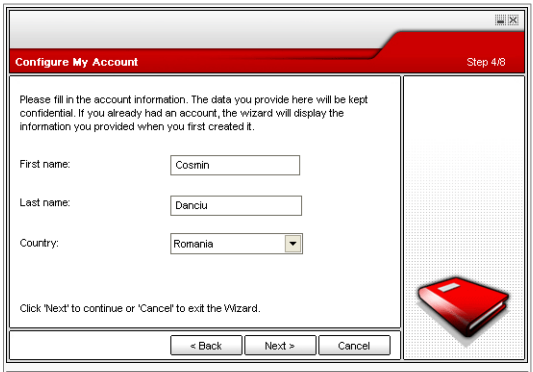
Tôi đã có tài khoản BitDefender

Nếu bạn đã có một tài khoản đang hoạt động, hãy cung cấp địa chỉ email và mật khẩu tài khoản của bạn. Nếu bạn cung cấp mật mã sai, bạn sẽ được chỉ dẫn cách đánh lại khi bạn nhấp chuột vào **Tiếp theot**. Nhấp **Ok** để enter lại mật mã hoặc **Cancel** để thoát wizard.

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

Click **Next** to continue or **Cancel** to exit the wizard.

2.3.4. Bước 4/8 - Vào các chi tiết tài khoản



Các chi tiết Tài khoản

Ghi chú
Bạn sẽ không đi qua được bước này nếu bạn chọn **Bỏ qua bước này** ở bước thứ ba.

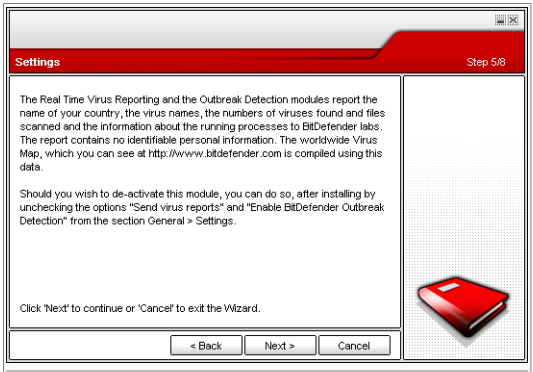
Điền họ và tên của bạn và chọn tên đất nước bạn đang cư trú.

Nếu bạn đã có một tài khoản, wizard sẽ hiển thị các thông tin bạn đã cung cấp trước đây nếu có. Tại đây, bạn có thể sửa các thông tin nếu như bạn muốn.

Quan trọng
Các dữ liệu bạn đã cung cấp sẽ được giữ bí mật.

Click **Next** to continue or **Cancel** to exit the wizard.

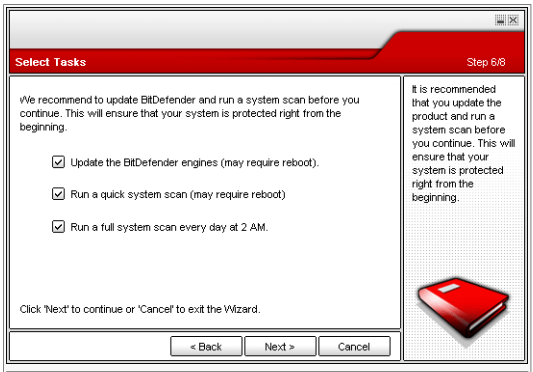
2.3.5. Bước 5/8 - Các thông tin về RTVR



Các thông tin về RTVR

Click **Next** to continue or **Cancel** to exit the wizard.

2.3.6. Bước 6/8 - Chọn Nhiệm vụ cần phải làm



Chọn Nhiệm vụ

Giao cho BitDefender Antivirus v10 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 Antivirus v10 engines (có thể cần phải khởi động lại)** - Trong bước tiếp theo, một hoạt động nâng cấp BitDefender Antivirus v10 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 Antivirus v10 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.

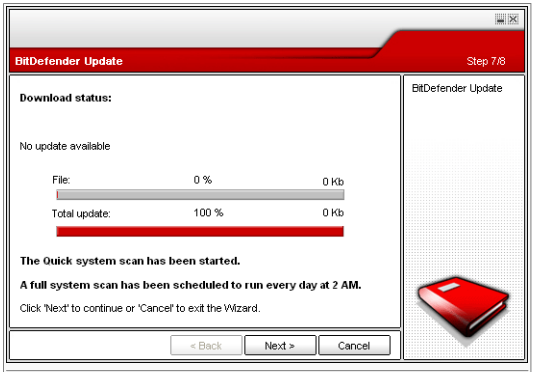
Quan trọng
Chúng tôi khuyến cáo bạn nên tạo khả năng cho các phương án này, trước khi chuyển sang bước tiếp theo để đảm bảo an toàn cho hệ thống của bạn.

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

Bạn có thể thay đổi bất cứ những gì bạn muốn bằng cách quay lại các bước trước đây(nhấp chuột vào **Back**). Sau đó, sẽ không thể quay lại quá trình này được nữa: Nếu bạn muốn tiếp tục thì bạn không thể quay lại các bước trước đây được nữa.

Click **Next** to continue or **Cancel** to exit the wizard.

2.3.7. Bước 7/8 - Hãy đợi để các nhiệm vụ được hoàn tất

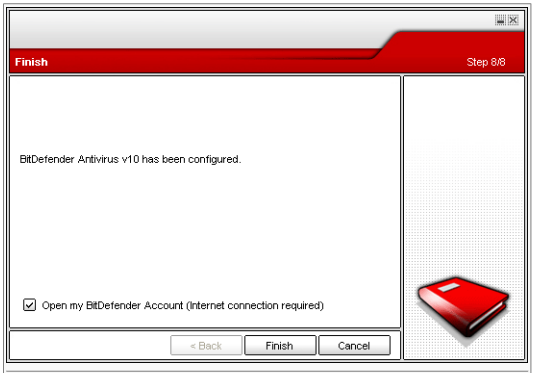


Tình trạng nhiệm vụ

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 **Next** to continue or **Cancel** to exit the wizard.

2.3.8. Bước 8/8 - Tóm tắt quan sát



Kết thúc

Đây là bước cuối cùng của wizard cấu hình.

Chọn **Mở tài khoản BitDefender của tôi**để vào tài khoản BitDefender của bạn. Cần nối mạng Internet.

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

2.4. 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, An ninh mạng bị loại trừ**

  Nhấp đúp thư mục cài đặt và theo chỉ dẫn (wizard) tại phần "*Các bước cài đặt*" (p. 9).

  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. 9).

  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.

2.5. Dỡ bỏ, sửa chữa và thay đổi các chức năng của BitDefender

Nếu bạn muốn thay đổi, sửa chữa hoặc dỡ bỏ **BitDefender Antivirus v10**, bạn hãy theo đường dẫn từ thực đơn khởi động của Windows **Start** → **Programs** → **BitDefender 10** → **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:

- **Thay đổi** - Để lựa chọn các phần mới của chương trình để bổ sung hoặc lựa chọn các phần hiện thời đã được lắp đặt rồi dỡ bỏ;
- **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 BitDefender settings. Sau khi quá trình sửa chữa kết thúc bạn có thể tải lại chúng.

- **Remove** - để dỡ bỏ tất cả các phần đã được cài đặt.

Để tiếp tục cài đặt, hãy chọn một trong ba phương án nêu trên. Chúng tôi đề nghị bạn chọn **Remove** để cho phần cài đặt lại được sạch sẽ. Sau khi quá trình không cài đặt kết thúc, chúng tôi khuyến cáo là bạn nên xoá đi tập tin `Softwin` ra khỏi `Program Files`.

Miêu tả và các đặc trưng

3. BitDefender Antivirus v10

Giải pháp phần mềm chống gián điệp và chống virus cho máy tính cá nhân của bạn!

BitDefender Antivirus v10là một công cụ chống gián điệp và chống virus rất mạnh với các tính chất đáp ứng tối đa các yêu cầu về an ninh của bạn. Sự dễ dàng sử dụng và nâng cấp tự động đã làm cho **BitDefender Antivirus** trở thành một sản phẩm 'cài rồi quên'.

3.1. Antivirus

Mục đích của module chống virus là đảm bảo việc phát hiện và diệt tất cả các virus. BitDefender Antivirus sử dụng các đầu quét mạnh được cấp chứng chỉ của ICSA Labs, Virus Bulletin, Checkmark, CheckVir và TÜV.

Phát hiện nhanh. B-HAVE (Tự phân tích hành vi trong các môi trường ảo) tạo một máy tính ảo nằm trong một máy tính thật nơi mà các bộ phận của phần mềm được chạy thử để phát hiện hành vi nguy hiểm tiềm tàng. Công nghệ độc quyền này của BitDefender tạo ra một tầng bảo vệ mới giữ cho hệ điều hành an toàn khỏi bị các virus lạ xâm phạm bằng cách phát hiện các bộ phận nguy hiểm của mã trong khi nó chưa được sưu tầm chữ ký định nghĩa virus.

Chống virus thường xuyên. Các đầu quét BitDefender mới và được cải tiến sẽ quét và làm sạch các tập tin bị nhiễm khi tiếp cận, giảm tối đa việc mất dữ liệu. Các tài liệu bị nhiễm virus được phục hồi thay vì bị xoá bỏ đi.

Phát hiện và diệt rootkit. Một module BitDefender mới tìm kiếm các rootkit (các chương trình nguy hiểm được thiết kế và ẩn nấp để khống chế các máy tính là nạn nhân) và tiêu diệt chúng khi phát hiện được.

Quét Web. Lưu lượng Web bây giờ được lọc đúng thời hạn, thậm chí được lọc trước khi chạm đến hộp thoại browser của bạn làm cho web an toàn.

Hàng ngang và Bảo vệ các ứng dụng nhắn tin. Các bộ lọc chống virus được lan truyền qua việc nhắn tin khẩn cấp và các ứng dụng phần mềm trao đổi tập tin.

Bảo vệ hoàn toàn Email. BitDefender chạy trên định ước chuẩn POP3/SMTP lọc tất cả các thư điện tử đến và đi cho dù bất cứ khách hàng là ai đã sử dụng (Outlook™, Outlook Express™, The Bat!™, Netscape®,...), không cần cấu hình bổ sung nào.

3.2. Chống gián điệp

BitDefender theo dõi và ngăn ngừa các hiểm hoạ gián điệp tiềm tàng đúng thời hạn, trước khi chúng có thể làm hư hại hệ thống của bạn. Bằng việc sử dụng một cơ sở dữ liệu toàn diện các chữ ký gián điệp nó sẽ bảo vệ cho máy tính của bạn khỏi phần mềm gián điệp.

Chống gián điệp tức thì. BitDefender theo dõi hàng chục "điểm nóng" trong hệ thống của bạn khi spyware có thể hoạt động và cũng kiểm tra bất cứ thay đổi nào trong hệ thống của bạn và trong phần mềm. Các hiểm hoạ gián điệp được nhận biết cũng được chặn đứng tức thì.

Quét và làm sạch các chương trình gián điệp. BitDefender có thể quét toàn bộ hệ thống của bạn hoặc chỉ một phần của hệ thống đối với các hiểm hoạ gián điệp đã được biết đến. Hệ thống quét sử dụng cơ sở dữ liệu được cập nhật về các chữ ký gián điệp.

Bảo vệ riêng tư. Bảo vệ bí mật cá nhân theo dõi lưu lượng HTTP (web) và SMTP (mail) đi ra từ máy tính của bạn có thể chứa các thông tin cá nhân như số thẻ tín dụng, số Bảo hiểm Xã hội, và các thông tin bí mật khác của người sử dụng (ví dụ như một phần của các mật khẩu).

Chống quay điện thoại. Một chương trình chống quay điện thoại được cấu hình để ngăn chặn các ứng dụng hiểm độc nhằm bắt bạn phải trả một hoá đơn điện thoại với số tiền lớn.

Kiểm soát Cookie. Phần mềm chống gián điệp lọc các tập tin đến và đi để giữ bí mật cá nhân, sở thích của bạn khi bạn đang lướt web trên Internet.

Kiểm soát nội dung tích cực. Chặn trước bất cứ ứng dụng nào có tiềm năng gây nguy hiểm như: các mã loại ActiveX, Java Applets or Java Scripts.

3.3. Các đặc điểm khác

Triển khai và sử dụng. Một cẩm nang (wizard) được cài sẵn khởi động ngay lập tức sau khi lắp đặt, giúp ngwif sử dụng lựa chọn những phần cài đặt phù hợp nhất, thực hiện một lịch quét và cung cấp đường dẫn nhanh đến việc đăng ký và kích hoạt sản phẩm.

Kinh nghiệm của người sử dụng. BitDefender thiết kế theo kinh nghiệm của người sử dụng, tập trung vào việc tạo điều kiện sử dụng dễ dàng và tránh sự lộn xộn. Kết quả là nhiều module của BidDefender v10 module đòi hỏi rất ít tương tác của người sử dụng, qua việc sử dụng một cách thuận lợi kỹ thuật tự động và học bằng máy.

Nâng cấp từng giờ. Bản sao BitDefender của bạn sẽ được cập nhật 24 lần một ngày trên Internet, trực tiếp qua Proxy Server. Sản phẩm có khả năng tự sửa chữa,

nếu cần thiết, bằng cách tải xuống các tập tin bị lỗi hoặc bị mất từ các máy chủ (Server) BitDefender.

24/7 Hỗ trợ. Được cung cấp trên mạng bởi các đại diện trợ giúp có chuyên môn cao và bằng cách tiếp cận một cơ sở dữ liệu trên mạng với các câu trả lời cho Các Câu hỏi Thường xuyên.

Đĩa cứu trợ. BitDefender Antivirus v10được cung cấp trên một đĩa CD có thể khởi động. đĩa CD này có thể được sử dụng để phân tích, sửa chữa và làm sạch virus cho một hệ thống bị tổn thương không khởi động được.

4. Các Module của BitDefender

BitDefender Antivirus v10 chứa đựng các module: **General**, **Antivirus**, **Antispyware** và **Update**.

4.1. Module Chung

BitDefender được cấu hình toàn diện để đảm bảo an ninh cao nhất.

Trong module General bạn có thể cấu hình mức an ninh và thực hiện các nhiệm vụ an ninh quan trọng. bạn có thể đăng ký sản phẩm của bạn và đặt hành vi tổng thể cho BitDefender.

4.2. Module chống virus

BitDefender bảo vệ bạn khỏi virus, các chương trình gián điệp và các chương trình nguy hiểm khác lọt vào hệ thống của bạn bằng cách quét các tập tin của bạn, các thư điện tử; các thông tin được tải trên mạng xuống và tất cả các nội dung khác khi chúng chạy vào hệ thống của bạn.

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

- On-access scanning - ngăn chặn các virus mới xâm nhập hệ thống của bạn như: các chương trình gián điệp và các chương trình nguy hiểm khác. Nó cũng còn được gọi là sự bảo vệ đúng lúc - các tập tin được quét khi người sử dụng tiếp cận chúng. BitDefender sẽ, ví dụ như, quét một tài liệu phần word để phát hiện những mối nguy hiểm đã được nhận biết trước khi bạn mở tài liệu ra vvà quét một thư điện tử khi bạn nhận. BitDefender quét "như bạn dùng file" - khi kích hoạt.
- Quét theo yêu cầu - phát hiện các virus, các chương trình gián điệp và các chương trình nguy hiểm khác 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.

4.3. Module Chống gián điệp

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.

4.4. Module nâng cấp

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. Bằng cách mặc định, BitDefender tự động kiểm tra để cập nhật hàng giờ.

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** .
- **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**.

Hơn nữa, đứng trên quan điểm can thiệp của người sử dụng, chúng ta có thể xem xét:

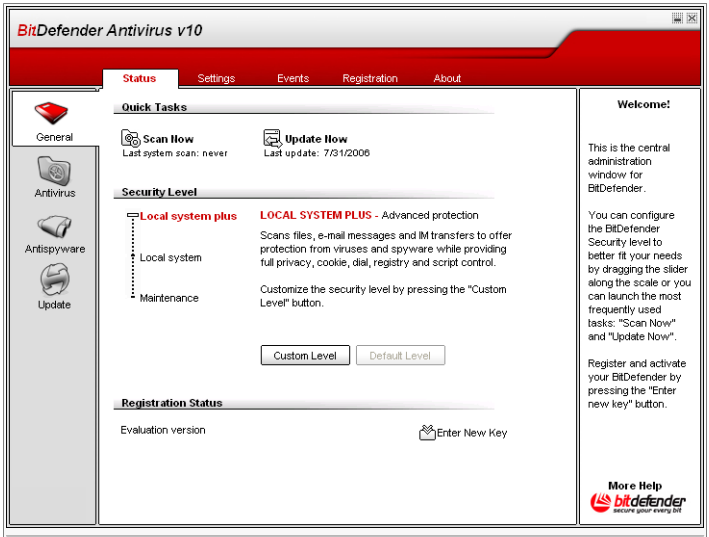
- Automatic update - BitDefender tự động tiếp xúc với server nâng cấp để kiểm tra xedm có chương trình nâng cấp mới nào ra đời hay không. Nếu có, BitDefender sẽ được tự động cập nhật. Viêc cập nhật tự động cũng có thể được tiến hành bất cứ lúc nào nếu như bạn nhấp chuột vào **Update now** từ module Update.
- Manual update - Bạn phải tự mình tải xuống và lắp đặt những chữ ký nguy hiểm mới nhất.

Bàn Quản lý

5. Tổng quan

BitDefender Antivirus v10 được thiết kế với console quản lý tập trung cho phép cấu hình của các phương án bảo vệ cho các module của BitDefender. Nói một cách khác tất cả những việc bạn cần phải làm là mở console quanr lý để có đường tiếp cận với tất cả các module: **Antivirus**, **Antispyware** và **Update**.

Để tiếp cận console quản lý,sử dụng thực đơn Start của Windows, bằng cách theo đường dẫn **Start** → **Programs** → **BitDefender 10** → **BitDefender Antivirus v10** hoặc để nhanh hơn nhấp đúp vào **BitDefender icon** từ ngăn hệ thống.



Bàn Quản lý

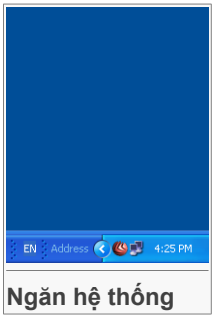
Ở phía trái console quản lý, bạn có thể nhìn thấy hộp thoại chọn module:

- General -Trong phần này, bạn có thể đặt mức bảo vệ an ninh tổng quát và thực hiện các nhiệm vụ an ninh thiết yếu. Tại đây, bạn cũng có thể đăng ký sản phẩm và xem phần tóm tắt của tất cả các danh mục chính được cài đặt của BitDefender, các chi tiết sản phẩm và thông tin tiếp xúc.
- Antivirus - Trong phần này, bạn có thể mặc định module **Antivirus**.
- Antispyware - Trong phần này, bạn có thể mặc định module **Antispyware**.
- Update - Trong phần này, bạn có thể mặc định module **Update**.

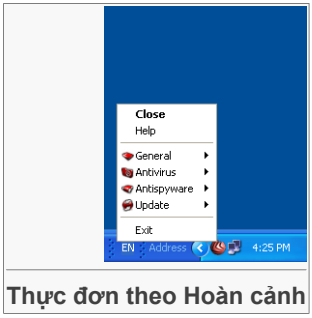
Ở phía bên phải của console quản lý, bạn có thể xem các thông tin về phần bạn đang ở trong đó. Phương án **More Help**, được đặt ở phía dưới bên phải, mở tập tin **Help**.

5.1. Ngăn hệ thống

Khi console mở ở mức tối thiểu, một biểu tượng sẽ xuất hiện trong ngăn hệ thống:



Ngăn hệ thống



Thực đơn theo Hoàn cảnh

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

- **Show / Close** - Mở console quản lý hoặc làm hiển thị ở mức tối thiểu thành ngăn hệ thống.
- **Help** - Mở tập tin trợ giúp.
- **General** - quản lý module General.
  - **Enter phím mới** - khởi động cẩm nang (wizard) đăng ký, hướng dẫn bạn trong suốt quá trình đăng ký.
  - **Sửa dữ liệu tài khoản** - khởi động cẩm nang giúp bạn tạo tài khoản BitDefender.
- **Antivirus** - quản lý module Antivirus.

- **có khả năng bảo vệ đúng lúc** - hiển thị tình trạng của bảo vệ đúng lúc (có khả năng / lhông có khả năng). Nhấp chuột vào phương án này để cho phép hoặc không cho phép bảo vệ đúng lúc.
- **Quét** - Mở một thực đơn phụ để từ đó bạn chó thể chọn để vận hành một trong các nhiệm vụ quét có tại phần Scan.

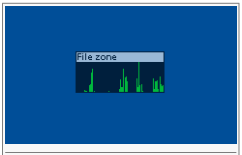
- **Chóng gián điệp** - Quản lý module Antispyware.
  - **Chóng gián điệo hành vi được cho phép / disabled** - hiển thị tình trạng của Bảo vệ -chống gián điệo hành vi (enabled / disabled). Nhấp chuột vào phương án này để cho phép hoặc không cho phép bảo vệ, chống gián điệp hành vi.
  - **Advanced settings** - Cho phép bạn định dạng các phần kiểm soát chống gián điệp.
- **Update** - Quản lý module Nâng cấp.
  - **Cập nhật ngay** - hãy tiến hành cập nhật ngay.
  - **Nâng cấp tự động được cho phép / không cho phép** - hiển thị tình trạng của nâng cấp tự động (được phép / không được phép). Nhấp chuột vào phương án này để cho phép hoặc không cho phép nâng cấp tự động.
- **Thoát** - Tắt ứng dụng này. Khi lựa chọn phương án này, biểy tượng từ ngăn hệ thống sẽ biến mất và để tiếp cận với console quản lý, bạn sẽ phải khởi động nó lại từ thực đơn khởi động của Windows.

Ghi chú

Biểu tượng sẽ biến thành màu đen nếu như bạn không cho phép một hoặc nhiều hơn module BitDefender. Bằng cách này, bạn sẽ biết liệu một số module có được phép hoạt động hay không mà không phải mở console quản lý.
Biểu tượng sẽ nhấp nháy khi đang cập nhật.

5.2. Thanh hoạt động quét

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



Thanh Hoạt động

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

Ghi chú

Thanh hoạt động quét sẽ thông báo cho bạn khi Virus Shield bị mất khả năng với một chữ thập đỏ trên khu vực tương ứng (**Vùng tập tin**). Bằng cách này bạ sẽ biết bạn có được bảo vệ không mà không cần phải mở console quản lý.

Khi bạn không muốn xem biểu tượng trực quan nữa, bạn chỉ cần nhấp chuột phải vào đó và chọn **Ẩn** .

Ghi chú
Để làm cửa sổ này biến đi hoàn toàn, hãy thoát khỏi **Cho phép thanh hoạt động quét (trên biểu đồ màn hình của hoạt động sảne phẩm)** phương án (từ module **General**, Settings section).

6. Module Chung

Phần **General** của cẩm nang cho người sử dụng này chứa các đề tài sau:

- Quản lý Trung tâm
- Cài đặt thanh quản lý
- các sự kiện
- Đăng ký sản phẩm
- Nói về

Ghi chú
Để có thêm chi tiết về module **General** module, hãy kiểm tra phần miêu tả của Phần 4.1, "*Module Chung*".

6.1. Quản lý Trung tâm

Quản lý Trung tâm

Trong phần này, bạn có thể cấu hình mức an ninh tổng quát và thực hiện các nhiệm vụ quan trọng của BitDefender. bạn cũng có thể đăng ký sản phẩm và xem ngày hết hạn.

6.1.1. Các nhiệm vụ nhanh

BitDefender cho phép tiếp cận nhanh với các nhiệm vụ an ninh thiết yếu. Sử dụng các nhiệm vụ này, bạn có thể làm cho BitDefender được cập nhật, quét hệ thống của bạn hay chặn lưu lượng tin.

Để quét toàn bộ hệ thống chỉ cần nhấp **Quét bây giờ**. cửa sổ quét sẽ xuất hiện và việc quét toàn bộ hệ thống sẽ được bắt đầu.

Quan trọng
Chúng tôi xin khuyến cáo là bạn cần vận hành chương trình quét toàn bộ hệ thống ít nhất mỗi tuần một lần.Để biết thêm chi tiết về các nhiệm vụ quét và quá trình quét, xin hãy kiểm tra phần Quét theo yêu cầutrong cẩm nang hướng dẫn sử dụng này.

Trước khi quét hệ thống của bạn, chúng tôi khuyến cáo bạn nên cập nhật BitDefender để nó có thể phát hiện ra các mối hiểm hoạ mới nhất. Để cập nhật BitDefender chỉ cần nhấp chuột vào **Nâng cấp bây giờ** . Đợi một vài giây cho quá trình nâng cấp hoàn tất hoặc tốt hơn là kiểm tra phần Update để xem tình trạng nâng cấp.

Ghi chú
Để biết thêm chi tiết, xin hãy kiểm tra phần Cập nhật Tự động của hướng dẫn sử dụng này.

6.1.2. Mức an ninh

Bạn có thể chọn mức anh ninh phù hợp hơn với yêu cầu bảo vệ của bạn. Kéo con trượt dọc theo mặt chia độ để đặt mức an ninh phù hợp.

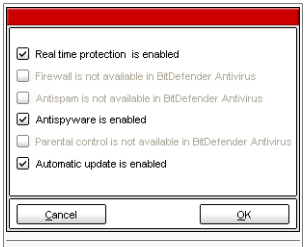
Có 3 mức an ninh:

Mức an ninh	Miêu tả
Bảo dưỡng	Không cung cấp chức năng bảo vệ. Chỉ có **Nâng cấp tự động** là có khả năng hoạt động. Chỉ cập nhật BitDefender. Mặc dù không có chức năng bảo vệ, mức an ninh này vẫn có thể hữu ích đới với người quản.
Hệ thống Cục bộ	Cung cấp chức năng phòng chống virus. Đặc biệt khuyến cáo để sử dụng cho các máy tính không có mạng công tác và không vào Internet. Mức tiêu thụ tài nguyên rất thấp. Các tập tin được tiếp cận được quét virus.
Thêm vào Hệ thống Cục bộ	Cung cấp các chức năng chống virus; chống gián điệp. Đặc biệt khuyến cáo để sử dụng cho các máy tính không có mạng công tác và không vào Internet. Mức tiêu thụ tài nguyên thấp.

Mức an ninh	Miêu tả
	Các tập tin được tiếp cận được quét virus và các chương trình gián điệp.

BitDefender Antivirus v10được khuyến cáo cho các máy tính không có mạng công tác và hoặc không vào Internet.

Bạn có thể tuỳ chỉnh mức an ninh bằng cách nhấp chuột vào **Custom level**. cửa sổ sau đây sẽ hiện ra:



Tuỳ chỉnh mức bảo vệ

Bạn có thể cho phép bất cứ phương án bảo vệ nào của BitDefender (**Bảo vệ đúng lúc** , **Chống gián điệp** , và **Nâng cấp Tự động** . Nhấp **OK**.

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

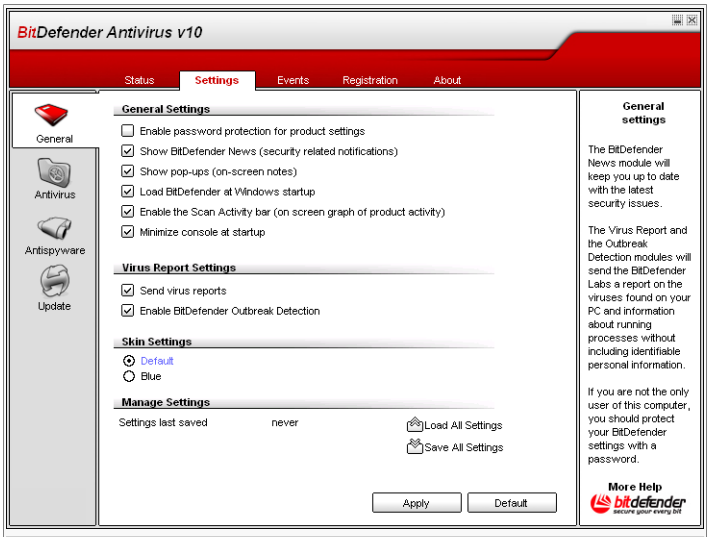
6.1.3. Tình trạng Đăng ký

Bạn có thể xem thông tin về tình trạng giấy phép BitDefender của bạn. Tại đây, bạn có thể đăng ký sản phẩm và xem thời gian hết hiệu lực.

Để enter một phím mới, nhấp chuột vào **Enter Phím mới**. Kết thúc cảm nang đăng ký để đăng ký thành công BitDefender.

Ghi chú
Để biết thêm chi tiết về quá trình đăng ký, xin hãy kiểm tra phần Đăng ký Sản phẩm của hướng dẫn sử dụng này.

6.2. Các phần cài đặt Console Quản lý



Các phần cài đặt Console Quản lý

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.

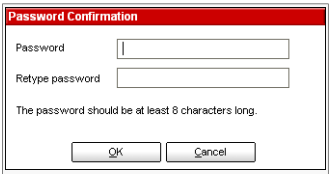
Có bốn phạm trù phương án: **cài đặt chung** , **Cài đặt thông báo Virus** , **Cài đặt lpứo bên ngoài** and **Quản lý cài đặt** .

6.2.1. Các phần cài đặt chung

- **Cho pheps bảo vệ mật mã để cài đặt sản phẩm** - Cho phép cài đặt một mật mã để bảo vệ cấu hình Console Quản lý của BitDefender Management;

Ghi chú
Nếu bạn khôg 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 mã.

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



Enter mật mã

Đánh mật mã vào trường **Password**, đánh lại vào trường **Đánh lại mật mã** và nhấp chuột vào **OK**.

Từ nay trở đi, nếu bạn muốn thay đổi các phương án cấn hình của BitDefender, bạn sẽ được yêu cầu trình báo mật mã.

Quan trọng
Nếu bạn quên mất mật mã, 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 nổ 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.

Ghi chú
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 .
- **Mở console ở mức tối thiểu khi khởi động** - Mở console quản lý BitDefender sau khi nó được tải tại phần khởi động hệ thống. Chỉ có BitDefender Icon sẽ xuất hiện trong ngăn hệ thống.

6.2.2. 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 nỗ 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.

6.2.3. Cài đặt lớp bên ngoài

Cho phép bạn chọn màu của console quản lý. Lớp bên ngoài là hình nền trênm giao diện. Để chọn lớp vỏ khác, hãy nhấp vào màu tương ứng.

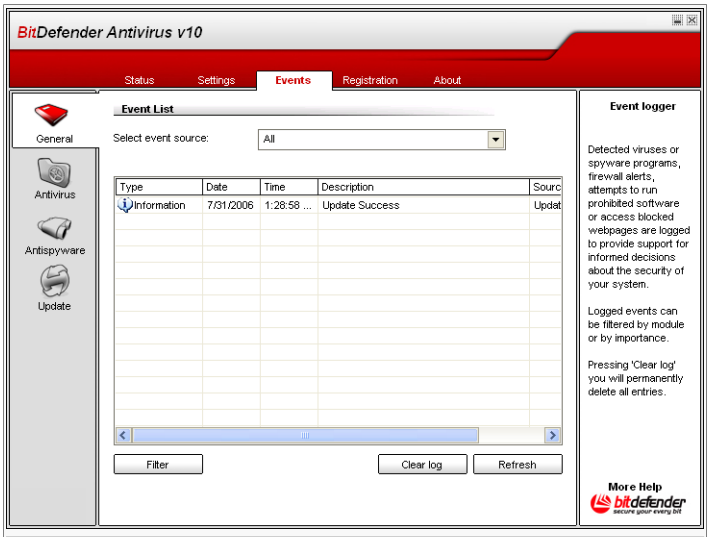
6.2.4. Quản lý cài đặt

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 phần cài đặt.

Nhấp **Apply** để lưu các thay đổi. Nếu bạn nhấp vào **Default** bạn sẽ tải được các phần cài đặt đã mặc định.

6.3. Các sự kiện



Các sự kiện

Trong phần này tất cả các sự kiện được xuất phát từ BitDefender được hiển thị.

Có tất cả ba loại sự kiện: **Information**, **Warning** và **Critical**.

Các ví dụ của các sự kiện:

- **Information** - Khi một thư điện tử được quét;
- **Cảnh báo** - khi một tập tin nghi ngờ bị phát hiện;
- **Critical** - khi một tập tin bị nhiễm virus được phát hiện.

Những thông tin sau đây được cung cấp cho mỗi sự kiện: ngày và giờ khi sự kiện diễn ra, một miêu tả ngắn và nguồn của nó (**Antivirus**, **Firewall**, **Chống gián điệp** or **Update**). Nhấp đúp chuột một sự kiện để xem các đặc tính của nó.

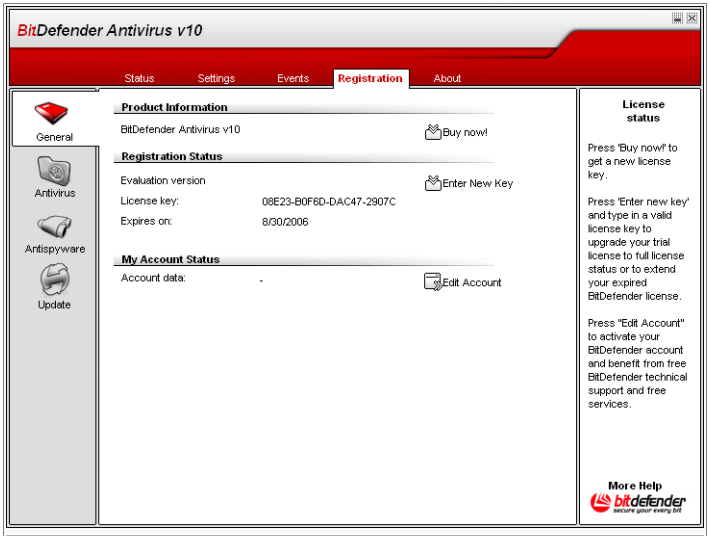
Bạn có thể lọc các sự kiện này theo hai cách (Bằng loại hoặc bàng nguồn):

- Click **Lọc** để chọn kiểu sự kiện nào để hiển thị.
- Chọn nguồn của sự kiện từ thực đơn rói bên dưới.

Nếu console quản lý mở tại phần **Events** và cùng lúc có một sự kiện xảy ra bạn phải nhấp vào **Làm mới** để xem sự kiện này.

Để xoá tất cả các sự kiện trong danh sách, nhấp vào **Bàn ghi Xoá** .

6.4. Đăng ký Sản phẩm



Đăng ký Sản phẩm

Phần này chứa đựng các thông tin về sản phẩm BitDefender (tình trạng đăng ký, số chứng minh của sản phẩm, ngày hết hạn) và tài khoản BitDefender. tại đây bạn có thể đăng ký sản phẩm và định dạng tài khoản BitDefender.

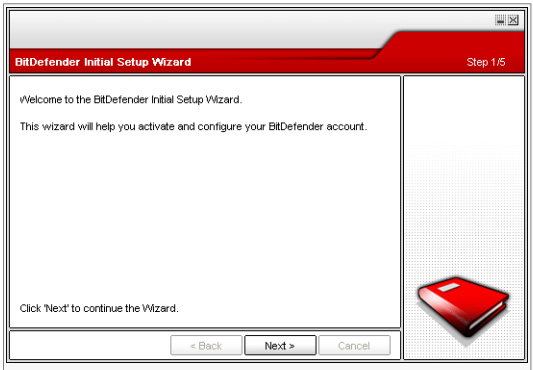
Nhấp vào nút **Mua bây giờ**để có đăng ký mới từ kho dự trữ trên mạng của BitDefender.

Bằng cách nhấp chuột vào **Enter phím mới** bạn có thể đăng ký sản phẩm, thay đổi khoá mới hoặc các chi tiết tài khoản. Để định dạng tài khoản BitDefender của bạn, hãy nhấp vào **Tài khoản Hiệu chỉnh** . Trong cả hai trường hợp, cẩm nang đăng ký sẽ xuất hiện.

6.4.1. Cẩm nang (Wizard) đăng ký

Thuật sĩ Đăng ký bao gồm 5 bước.

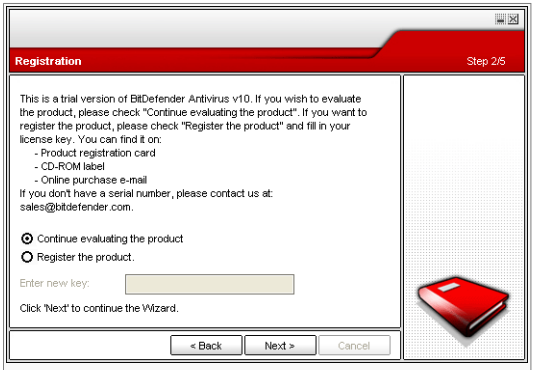
Bước 1/5 - Chào mừng bạn đến với Cẩm nang Đăng ký của BitDefender



Cửa sổ chào đón

Nhấp chuột vào **Next**.

Bước 2/5 - Đăng ký BitDefender



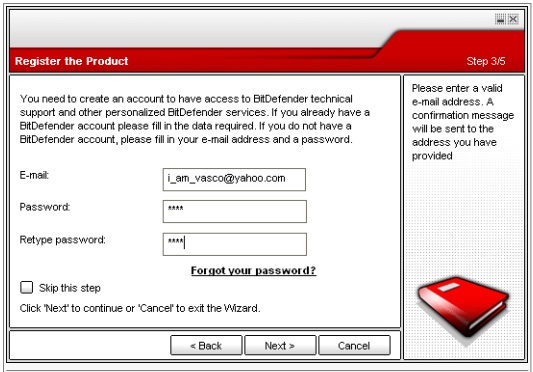
Đăng ký

Chọn **Đăng ký sản phẩm**để đăng ký **BitDefender Antivirus v10**. Đánh chìa khoá của giấy phép vào **Enter new key** field.

Tiếp tục đánh giá sản phẩm, xin chọn **Tiếp tục đánh giá sản phẩm,** .

Nhấp chuột vào **Next**.

Bước 3/5 -Lập 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.

Đánh địa chỉ email đang còn hiệu lực vào **E-mail** field. Nhớ mật mã và đánh 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 mã phải có ít nhất bốn ký tự.

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.

Quan trọng
Xin hãy kích hoạt địa chỉ email trước khi chuyển sang các bước tiếp theo.

Nếu bạn không muốn tạo ra một tài khoản BitDefender, bạn chỉ cần chọn **Bỏ qua bước này**. Bạn cũng sẽ bỏ qua bước tiếp theo của cẩm nang hướng dẫn (wizard).

Nhấp **Tiếp theot**để tiếp tục.

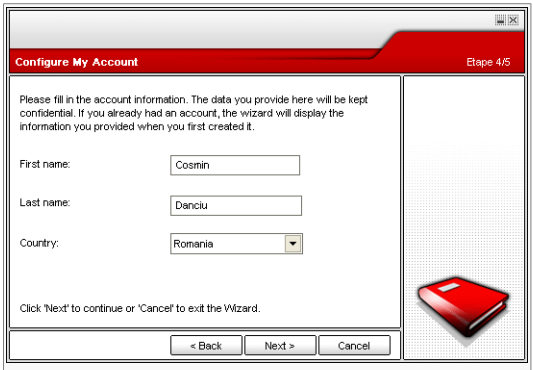
Tôi đã có tài khoản BitDefender

Nếu bạn đã có một tài khoản đang hoạt động, hãy cung cấp địa chỉ email và mật khẩu tài khoản của bạn. Nếu bạn cung cấp mật mã sai, bạn sẽ được chỉ dẫn cách đánh lại khi bạn nhấp chuột vào **Tiếp theot**. Nhấp **Ok** để enter lại mật mã hoặc **Cancel** để thoát wizard.

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

Nhấp **Tiếp theot**để tiếp tục.

Bước 4/5 - Enter cá chi tiết tài khoản



Các chi tiết Tài khoản

Ghi chú
Bạn sẽ không đi qua bước này nếu như bạn chọn **Bỏ qua bước này** trong bước thứ ba .

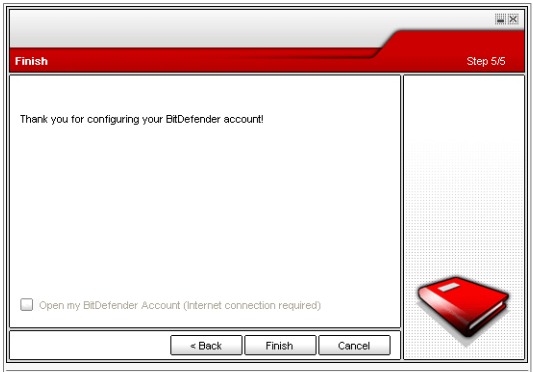
Hãy điền họ, tên và chọn nước của bạn.

Nếu bạn đã có một tài khoản, cẩm nang sẽ hiển thị thông tin trước đây bạn đã cung cấp, nếu có. Tại đây bạn có thể sửa lại các thông tin nếu như bạn muốn.

Quan trọng
Các dữ liệu bạn đã cung cấp sẽ được giữ bí mật.

Nhấp chuột vào **Next**.

Bước 5/5 - Tóm tắt Tổng quan



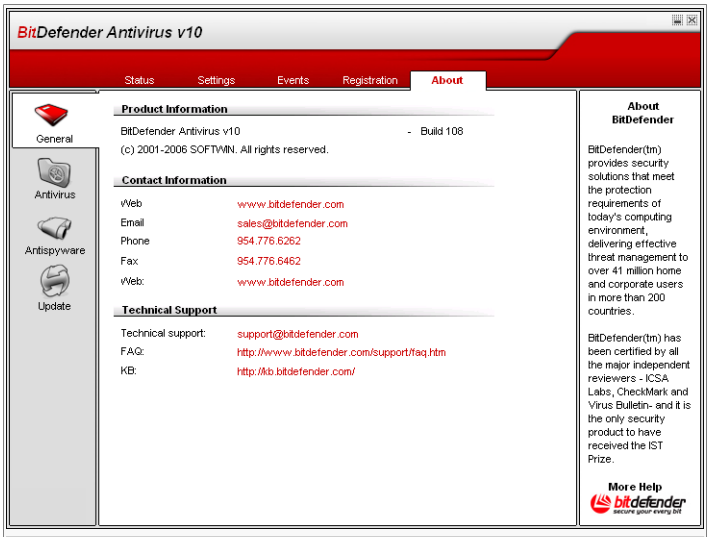
Kết thúc

Đây là bước cuối cùng của cẩm nang định cấu hình. Bạn có thể thay đổi bất cứ những gì bạn muốn bằng cách quay lợi các bước trước đó (nhấp chuột vào **Quay lại**).

Nếu bạn không muốn thay đổi bất cứ điều gì, hãy nhấp chuột vào **Kết thúc** để thoát ra khỏi cẩm nang.

Chọn **Mở tài khoản BitDefender của tôi**để vào tài khoản BitDefender của bạn. Cần nối mạng Internet.

6.5. Về



Thông tin chung

Trong phần này, bạn có thể tìm thông tin để liên lạc và các chi tiết của sản phẩm.

BitDefender™ cung cấp các giải pháp an ninh để đáp ứng các yêu cầu bảo vệ cho môi trường máy tính ngày nay, quản lý có hiệu quả các mối đe doạ cho hơn 41 triệu máy tính cá nhân và của công ty trên hơn 180 nước.

BitDefender™được cấp chứng chỉ của các nhà thẩm định độc lập tầm cỡ - **ICSA Labs**, **CheckMark** và **Bản tin Virus** , và là sản phẩm an ninh duy nhất giành được giải thưởng **IST** .

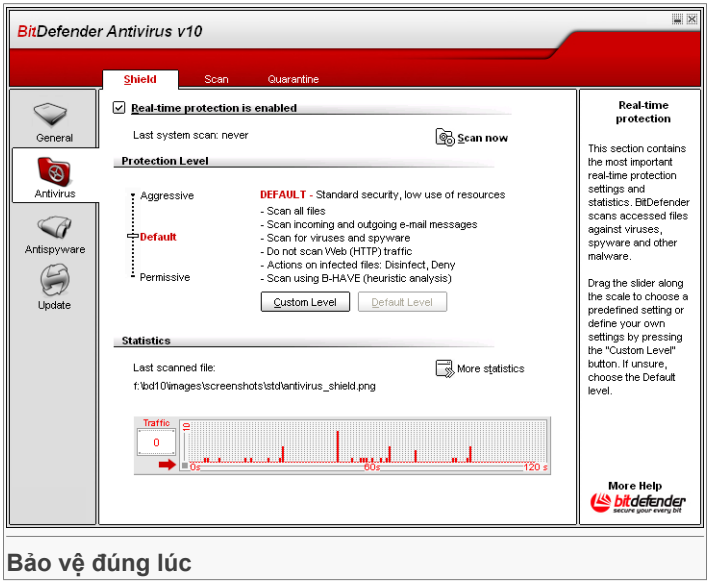
7. Module chống virus

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

- Quét khi truy cập
- Quét theo yêu cầu
- Kiểm dịch

Ghi chú
Để biết thêm chi tiết về module **Antivirus** xin hãy kiểm tra mô tả về Phần 4.2, "*Module chống virus*".

7.1. Quét khi truy cập



Bảo vệ đúng lúc

Tronng phần này bạn có thể định cấu hình **Bảo vệ đúng lúc** và bạn có thể xem thông tin về hoạt động của nó. **Real-time protection**sẽ bảo vệ cho máy tính của bạn an toàn bằng cách quét các thư điện tử, các thông tin được tải và các tập tin được truy cập.

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.

7.1.1. Mức bảo vệ

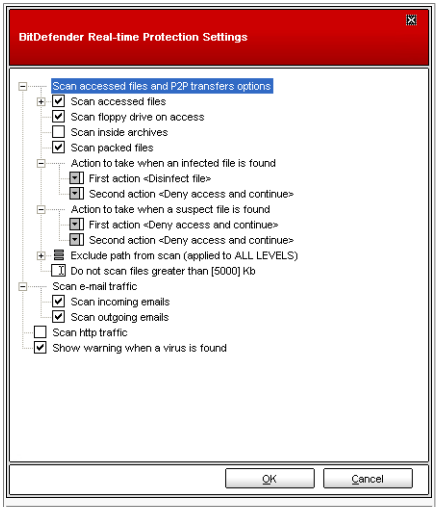
Bạn có thể chọn mức bảo vệ phù hợp hơn với các yêu cầu an ninh của bạn. Hãy kéo thanh trượt dọc theo mặt chia độ để chọn mức bảo vệ phù hợp.

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.

Những người sử dụng có trình độ cao có thể muốn tận dụng các lợi thế của các phần cài đặt quét do BitDefender cung cấp. Máy quét có thể được lắp đặt để bỏ qua các phần mở rộng tập tin, các thư mục hoặc các tài liệu lưu trữ mà bạn biết rõ là chúng vô hại. 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 án khám phá (exploring) của Windows.

Nhấp vào hộp có "+" để mở một phương án hoặc vào hộp có "-" để đóng một phương án.

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 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.

Phương án		Miêu tả
	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 ";".
	Không quét phần mở rộng: [ ]	Các tập tin với những phần mở rộng được người sử dụng chỉ ra sẽ KHÔNG được quét. Những phần mở rộng này phải được tách ra bằng ";".
	Quét cho phần có nguy cơ	Quét cho phần có nguy cơ. Những tập tin này sẽ được xử lý như những tập tin bị nhiễm. Phần mềm bao gồm các thành tố bổ sung có thể ngừng làm việc nếu như cho phép phương án này hoạt động. Chọn **Bỏ qua, không quét dialers và các ứng dụng** nếu bạn muốn bỏ qua, không quét các tập tin thuôvj loại này.
Scan floppy drive on access		Quét ổ đĩa mềm khi nó đang được truy xuất.
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.
	Chuyển đến nơi kiểm dịch	Chuyển các tập tin bị nhiễm đến nơi kiểm dịch.
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.

Phương án	Miêu tả
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 nơi kiểm dịch.
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.
Bỏ không quét (áp dụng cho TẤT CẢ CÁC CẤP ĐỘ)	Nhấp vào "+\ tương ứng với phương án này để xác định thư mục sẽ được loại trừ không quét. Hậu quả của việc này là phương án sẽ được mở rộng và một phương án mới `New item`, sẽ xuất hiện. Nhấp vào hộp thoại kiểm tra tương ứng của danh mục mới và từ exploring window, hãy chọn thư mục mà bạn muốn loại ra, không quét. Các đối tượng được chọn ở đây sẽ được loại trừ, không quét cho dù mức bảo vệ có được chọn đi nữa (không chỉ đối với **Mức Thông dụng**).

- **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.

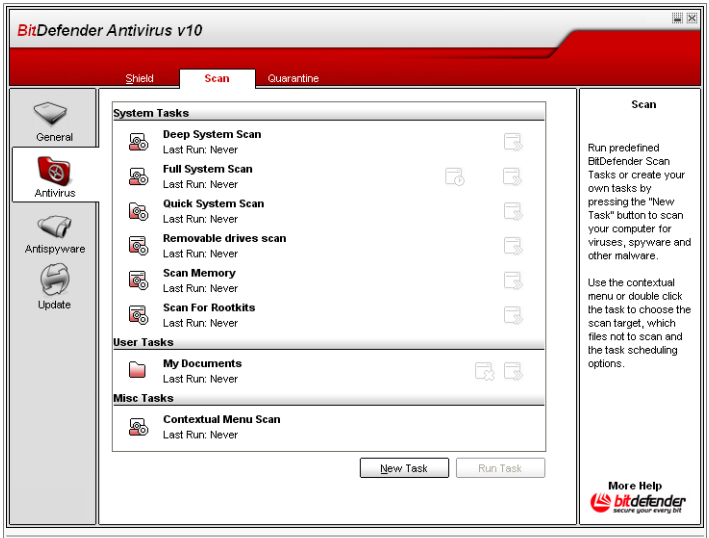
  Đối với một tập tin bị nhiễm, cửa sổ cảnh báo sẽ chứa tên của virus,đường dẫn đến virus đó và hành động của BitDefender và đường kết nối với vị trí của BitDefender, nơi bạn có thể tìm thấy thêm thông tin về nó. Đối với một thư điện tử bị nhiễm, cửa sổ cảnh báo cũng sẽ chứa các thông tin về người gửi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

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

Nếu bạn muốn quy trở về mức mặc định, hãy nhấp **Mức Mặc định** .

7.2. Quét theo yêu cầu



Các nhiệm vụ quét

Trong phần này, bạn có thể cấu hình BitDefender để quét máy tính của bạn.

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.

7.2.1. Các nhiệm vụ quét

Quét theo yêu cầu được dựa trên các nhiệm vụ quét.Người sử dụng có thể quét máy tính, sử dụng các nhiệm vụ mặc định hoặc các nhiệm vụ quét của mình (Các nhiệm vụ người sử dụng xác định).

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 toàn bộ hệ thống, kể cả lưu trữ, để tìm virus và gián điệp.
Quét toàn bộ hệ thống	Quét toàn bộ hệ thống, trừ lưu trữ, để tìm virus và gián điệp.
Quét nhanh Hệ thốngQuick System Scan	Quét tất cả các chương trình để tìm virus và các phần mềm gián điệp.
Quét ổ đĩa lưu động	Quét các ổ đĩa lưu động để tìm virus và các phần mềm gián điệp.
Quét bộ nhớ	Quét bộ nhớ để tìm các mối đe doạ gián điệp đã được biết đến.
Quét tìm các công cụ Gốc	Quét bộ nhớ để tìm các chương trình vụng trộm.

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

  Một nhiệm vụ có tên là `Tài liệu của tôi` được cung cấp. Sử dụng nhiệm vụ này để quét các tài liệu của bạn từ thư mục `Tài liệu của tôi` .

- **Các nhiệm vụ hỗn hợp** - Chưa sdanh 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.

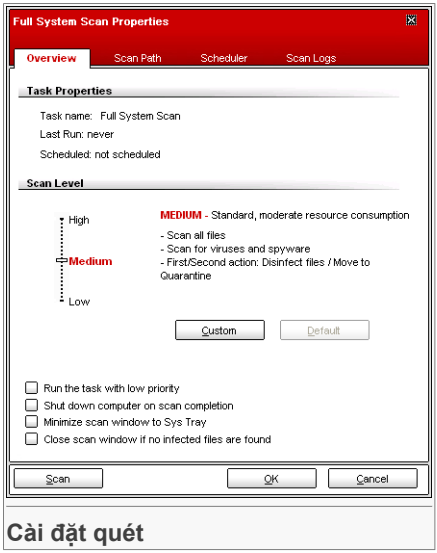
Ghi chú
Không có đối các nhiệm vụ hệ thống. Bạn không thể huỷ bỏ một nhiệm vụ hệ thống.

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

7.2.2. Các đặc tính của Nhiệm vụ Quét

Mỗi nhiệm vụ quét có cửa sổ của mình **Đặc điểm** nơi bạn có thể định hình các phương án quét, hãy đặt mục tiêu quét, lập kế hoạch cho nhiệm vụ hoặc xem các báo cáo. Để enter cửa sổ này, hãy nhấp đúp vào nhiệm vụ. Cửa sổ sau đây sẽ xuất hiện:

Cài đặt quét



Cài đặt quét

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.

Mức quét

Trước tiên, bạn cần phải chọn mức quét. Kéo con trượt dọc theo bảng chia độ để đặt mức 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 tìm virus. Ngoài việc quét dựa trên chữ ký cổ điển, phép phân tích theo kinh nghiệm cũng được sử dụng. Các hành động được áp dụng cho các tập tin bị nhiễm là: làm sạch tập tin/ gửi tới nơi kiểm dịch.
Trung bình	Cung cấp hiệu suất phát hiiện tốt. Mức tiêu thụ tài nguyên trung bình. Tất cả các tập tin đều được quét để tìm virus và các phần mềm gián điệp. Ngoài việc quét dựa trên chữ ký cổ điển, phép phân tích theo kinh nghiệm cũng được sử dụng. Các hành động được áp dụng cho các tập tin bị nhiễm là: làm sạch tập tin/ gửi tới nơi kiểm dịch.
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 để tìm virus và các phần mềm gián điệp. Ngoài việc quét dựa trên chữ ký cổ điển, phép phân tích theo kinh nghiệm cũng được sử dụng. Các hành động được áp dụng cho các tập tin bị nhiễm là: làm sạch tập tin/ gửi tới nơi kiểm dịch.

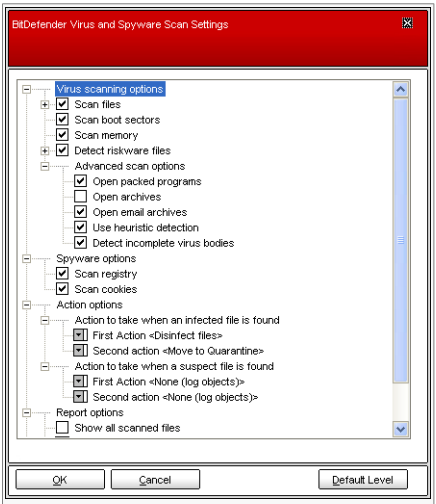
Quan trọng

Quét tìm các Rootkit Nhiệm vụ có cùng mức quét. Song, các phương án lại khác:

- **Thấp** - Chỉ có các quá trình được quét. Không có hành động nào được tiến hành đối với các đối tượng được phát hiện.
- **Trung bình** - Các tập tin và các quá trình được quét để tìm những đối tượng lẩn trốn. Không có hành động nào được tiến hành đối với các đối tượng được phát hiện.
- **Cao** - Các tập tin và các quá trình được quét để tìm những đối tượng lẩn trốn. Các đối tượng bị phát hiện được đặt tên lại.

Những người sử dụng có trình độ cao có thể muốn khai thác các lợi thế của những phần cài đặt quét do BitDefender mang lại Máy quét có thể được đặt để bỏ qua các phần mở rộng của tập tin, các thư mục, các tài liệu lưu trữ mà bạn biết rõ là chúng vô hại. Việc này có thể làm giảm đáng kể thời gian quét và cải thiện toính thức ứng của máy tính trong quá trình quét.

Click **Tuỳ chỉnh** để đặt các phương án quét của mình. cửa sổ sau đây 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 án khám phá (exploring) của Windows.

Các phương án quét được nhóm thành năm phạm trù:

- **Các phương án quét virus**
- **Các phương án gián điệp**
- **Các phương án hành động**
- **Các phương án Báo cáo**
- **Các phương án khác**

Nhấp vào hộp có "+" để mở một phương án hoặc vào hộp có "-" để đóng một phương án.

Quan trọng

Đối với nhiệm vụ **Quét để tìm Rootkit** chỉ có ba phạm trù: **Các phwong án quét Rootkit** , **Các phương án Báo cáo** và **Các phương án khác** . Từ phạm trù thứ nhất, bạn có thể chọn những gì để quét (các tập tin hoặc bộ nhơ, hoặc cả hai) avà bạn có thể đưa ra hành động cho các đối tượng bị phát hiện (**Không (Ghi các đối tượng vào nhật ký)/Đổi tên tập tin**). Hai phạm trù cuối cùng đồng nhất với các phạm trù được miêu tả dưới đây.

- 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.

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; 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 ";".
	Loại trừ các phần mở rộng do người sử dụng xác định	Các tập tin với những phần mở rộng được người sử dụng chỉ ra sẽ KHÔNG được quét. Những phần mở rộng này phải được tách ra bằng ";".
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.
phát hiện các tập tin có nguy cơ lây nhiễm		Quét các mối đe doạ khác ngoài virus như dialers và adware. Những tập tin này sẽ được xử lý như những tập tin bị nhiễm. Phần mềm chứa các thành phần của adware có thể ngừng làm việc nếu như phương án này hoạt động. Chọn **Trừ các ứng dụng và các dialer** Nếu bạn muốn loại trừ không quét các tập tin này.
Các phương án quét cao cấp	**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.

Phương án	Miêu tả
Sử dụng phương pháp phát hiện theo kinh nghiệm	Để sử dụng phương pháp quét các tập tin bằng kinh nghiệm. Mục đích của việc quét bằng kinh nghiệm là để xác định những virus mới, dựa trên các kiểu, dạng, các thuật toán nhất định, trước khi tìm ra định nghĩa 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.
phát hiện các thực thể virus chưa hoàn thiện	Phát hiện các thực thể virus chưa hoàn thiện.

- Xác định mục tiêu quét các chương trình gián điệp (registry, cookies). Thực hiện việc này bằng cách chọn một số phương án từ phạm trù **Các phương án quét các chương trình gián điệp** .

Phương án	Miêu tả
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 hoặc bị nghi ngờ. Mở phạm trù **Action options** để xem tất cả các hành động có thể tiến hành đối với các tập tin này.

  Chọn hành động phải tiến hành khi một tập tin bị nhiễm hoặc bị nghi ngờ được phát hiện ra.Bạn có thể chỉ rõ các hành động khác nhau đối với các tập tin bị nhiễm hay bị nghi ngờ. Bạn cũng có thể chọn hành động thứ hai nếu như hành động đầu thất bại.

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.

Hành động	Miêu tả
Chỉ dẫn cho người sử dụng phải hành động như thế nào	Khi một tập tin bị nhiễm được phát hiện, một cửa sổ sẽ xuất hiện chỉ dẫn cho người sử dụng cách chọn hành động cho tập tin đó. Tuỳ thuộc vào tầm quan trọng của tập tin, bạn có thể chọn cách diệt virus, cách ly tại vùng kiểm dịch hoặc xoá bỏ nó đi.
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 Kiểm dịch.
Đổi tên các tập tin	Thay đổi phần mở rộng của các tập tin bị nhiễm. Phần mở rộng mới của các tập tin bị nhiễm là `.vir`. Bằng cách đổi tên các tập tin bị nhiễm, khả năng hoạt động và khả năng lây lan của chúng sẽ bị mất đi. Đồng thời, chúng sẽ được lưu lại cho việc giám định và phân tích tiếp theo.

Quan trọng

Thay đổi tên của các tập tinRename files có hiệu quả tương tự đối với các tập tin ẩn (rootkits). Phần mở rộng mới của các tập tin bị phát hiện sẽ là `.bd.ren`. Bằng cách đổi tên các tập tin bị nhiễm, khả năng hoạt động và khả năng lây lan của chúng sẽ bị mất đi. Đồng thời, chúng sẽ được lưu lại cho việc giám định và phân tích tiếp theo.

- Hãy chỉ rõ các phương án cho các tập tin báo cáo. Mở phạm trù **Report options** để xem tất cả các phương án có thể.

Phương án	Miêu tả
Hiển thị tất cả các file được quét	Liệt kê tất cả các tập tin đã được quét và tình trạng của chúng (bị nhiễm hay không) trong tập tin báo cáo. Khi phương án này mở, máy tính sẽ chạy chậm lại.
Xoá các logs đã tồn tại lâu hơn [x] ngày	Đây là một trường hiệu chỉnh, nó cho phép chỉ rõ một báo cáo sẽ được giữ trong thời gian bao lâu trong phần Quét Logs. Chọn phương án này và đánh vào khoảng cách thời gian mới. Khoảng cách thời gian mặc định là 180 ngày.

Ghi chú
Có thể xem các tập tin báo cáo trong phần Scan Logstừ cửa sổ **Các đặc điểm**.

- Chỉ rõ các phương án khác. Mở phạm trù **Other options**, từ đây bạn có thể chọn phương án sau:

Phương án	Miêu tả
Hãy gửi tập tin bị nghi ngờ đến phòng thí nghiệm của BitDefender Lab	Bạn sẽ được chỉ dẫn cách gửi tất cả các tập tin bị nghi ngờ đến phòng thí nghiệm của BitDefender lab sau khi qú trình quét kết thúc.

Nếu bạn nhấp vào **Mức Mặc định** bạn sẽ tải được các phần cài đặt đã được mặc định.

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

Các phần cài đặt khác

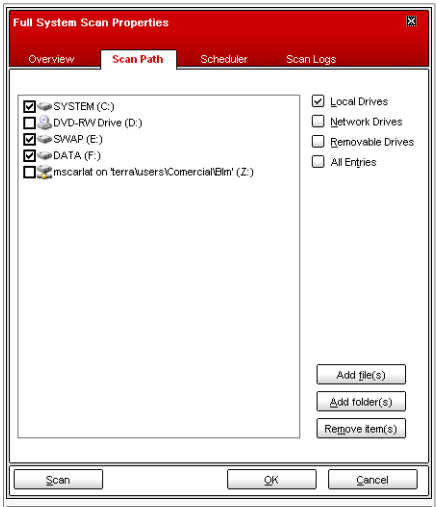
Một loạt các phương án chung cho quá trình quét cũng đựoc hiện diện:

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.
Tắt PC quét xong	Tắt máy tính khi quá trình quét kết thúc.
Hãy gửi tập tin bị nghi ngờ đến phòng thí nghiệm của BitDefender Lab	Bạn sẽ được chỉ dẫn cách gửi tất cả các tập tin bị nghi ngờ đến phòng thí nghiệm của BitDefender lab sau khi qú trình quét kết thúc.
Mở cửa sổ quét ở mức tối thiểu khi khởi động ngăn hệ thống	Mở cửa sổ quét ở mức tối thiểu tới ngăn hệ thống . Nhấp đúp vào biểu tượng BitDefender icon để mở.

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

Mục tiêu quét

Nhấp đúp vào nhiệm vụ được chọn và sau đó nhâls vào tab **Scan Path**để vào phần này.



Mục tiêu quét

Tại đây, bạ có thể đặt mục tiêu quét.

Phần này chứa các nút sau:

- **Bổ sung các tập tin** - mở một cửa sổ duyệt qua, tại đây bạn có thể chọn các tập tin mà bạn muốn quét.
- **Bổ sung các tập tin** - giống như trên nhưng bạn chọn các thư mục bạn muốn BitDefender quét thay vì chọn các tập tin.

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

- **Loại bỏ các mục** - Loại bỏ các tập tin/các thư mục mà trước đây đã được chọn từ danh mục 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.

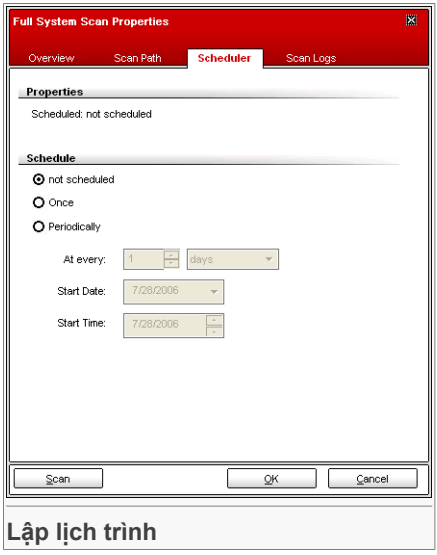
- **Các ổ đĩa nội bộ** - Để quét các ổ đĩa nội bộ.
- **Các ổ đĩa của mạng công tác** - Để quét các ổ đĩa của mạng công tác.
- **Các ổ đĩa lưu động** - Để quét các ổ đĩa lưu động (CD-ROM, đĩa mềm).
- **Tất các các cổng vào** - để quét tất cả các ổ đĩa, cho dù chúng là ổ đĩa nội bô, mạng công tác hay lưu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

Ghi chú
Nếu bạn muốn quét toàn bộ máy tính để tìm virus, bạn hãy chọn hộp kiểm tra tương ứng với **Tất cả các cổng vào**.

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

Lập lịch trình

Nhấp đúp vào một nhiệm vụ được chọn và sau đó nhấp voà phím tab **Scheduler** để vào phần này.



Lập lịch trình

Tại đây bạn có thể thấy nhiệm vụ đã được lên kế hoạch chưa và bạn có thể sửa đổi các đặc điểm này.

Quan trọng
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.

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

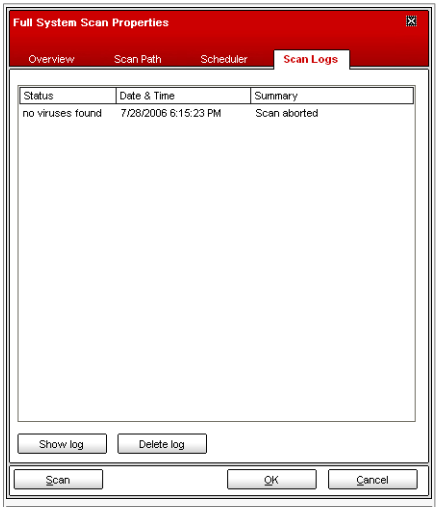
- **Không được lên kế hoạch** -Khởi động nhiệm vụ chỉ khi nào có yêu cầu của người sử dụng.
- **Once** -Bắt đầu quét chỉ một lần tại một thời điểm nhất định. Nêu cụ thể ngày tháng và thời gian bắt đầu tại các trường emphasis role="bold">Ngày tháng bắt đầu /Thời gian/emphasis>.
- **Định kỳ** - Khởi động 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**.

Quét các bản ghi

Nhấp đúp vào một nhiệm vụ đượcc chọn rồi sau đó nhấp vào phím tab **Scan Logs** để vào phần này.



Quét các bản ghi

Tại đây bạn có thể nhìn thấy các tập tin báo cáo nảy sinh mỗi khi có một nhiệm vụ được thực hiện. Mỗi tập tin có đính kèm các thông tin về tình trạng của nó (sạch/bị nhiễm),ngày, giờ lúc việc quét được thực hiện và tóm tắt (Hoạt động quét kết thúc).

Có hai nút:

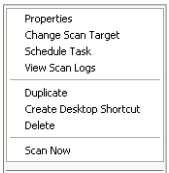
- **Hiển thị bản ghi** - để xem tập tin báo cáo được lựa chọn;
- **Xoá bản ghi** - để xoá tập tin báo cáo được chọn.

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**.

7.2.3. Thực đơn tắt

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



Thực đơn tắt

Các liệnh sau đây có sẵn trên thực đơn tắt:

- **Các đặc điểm** - mở cửa sổ **Các đặc điểm**, **Tổng quan** tab, tại đây bạn có thể thay đổi các phần cài đặt của nhiệm vụ được chọn;
- **Thay đổi Mục tiêu Quét** - Mở cửa sổ **Các đặc điểm** , **Scan Path** tab, tại đây bạn có thể thay đổi mục tiêu quét cho nhiệm vụ được chọn;
- **Nhiệm vụ lập kế hoạch** - mở cửa sổ **Properties**, **Scheduler** tab, tại đây, bạn có thể lập kế hoạch cho mộ nhiệm vụ được chọn;
- **View Scan Logs** - Mở cửa sổ **Properties**, **Phiám tab Quét các bản ghi** 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.

- **Tạo đường tắt cho Màn hình nền** - tạo ra một lối tắt của màn hình nền cho nhiệm vụ được chọn;
- **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.

- **Quét bây giờ** - vận hành hoạt động được chọn, khởi xướng một hành động quét ngay lập tức.

Quan trọng
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** .

7.2.4. Các kiểu quét theo yêu cầu

BitDefender cho phép ba 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 v10;
- Drag& Quét thả -kéo và thả một tập tin hoặc một thư mục trên Thanh hoạt động Quét ;

Quét ngay lập tức

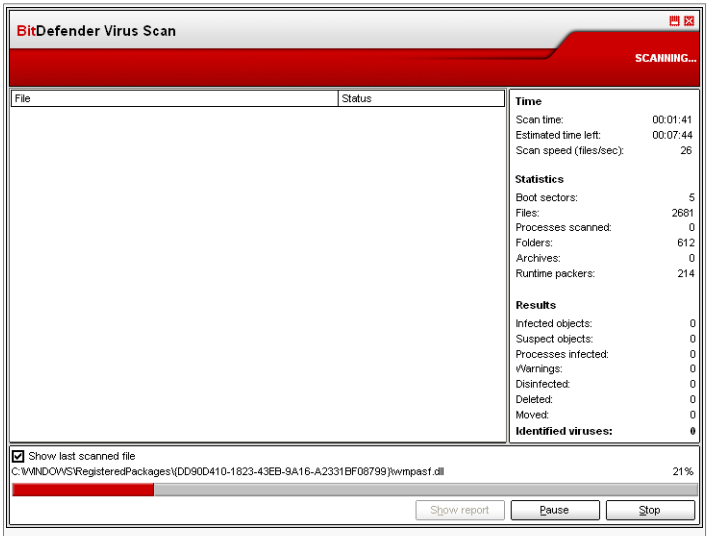
Để quét toàn bộ hay quét mộy phần của máy tính, bạn có thể sử dụng các nhiệm vụ quét mặc định hoặc bạn có thể tự tạo ra các nhiệm vụ quét của mình.Có hai phương pháp tạo ta các nhiệm vụ quét:

- Nhân bản một nhiệm vụ hiện hành, đổi tên nhiệm cụ đó và tạo các thay đổi cần thiết trong cửa sổ Các đặc điểm ;
- Click **New Task** to create a new task and configure it.

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.

Trước khi cho BitDefender quét máy tính của bạn, bạn cần phải chắc chăn rằng BitDefender đã được cập nhật tấtc cả các chữ ký của virus,bởi vì các virus mới được tìm và xác định hàng ngày. Bạn có thể xác định xem lần cập nhật gần nhất là lúc nào ở phía trêb của module Nâng cấp .

Để bắt đầu quét, chỉ cần chọn nhiệm vụ quét bạn muốn từ danh sách và nhấp vào nút phía bên phải **Quét bây giờ**. Bạn cũng có thê nhấp vào **Run Task**. Một cửa sổ quét sẽ hiện ra:



Cửa sổ quét

Một biểu tượng sẽ xuất hiện tại ngăn hệ thống khi quá trình quét vận hành.

Khi quét, BitDefender sẽ chỉ cho bạn quá trình quét và cảnh báo bạn khi tìm thấy bất cứ mối đe doạ nào. Tuỳ thuộc vào nhiệm vụ quét, sẽ có thông tin về các chương trình gián điệp và/hoặc các virus. Nếu có cả hai loại thônbg tin đó, nhấp vào phím tương ứng để biết thêm chi tiết về quá trình quét gián điệp hoặc virus.

Chọn hộp kiểm tra tương ứng với **Hãy chỉ ra tập tin được quét lần cuối cùng** và chỉ có các thông tin về tập tin được quét lần cuối cùng được hiển thị.

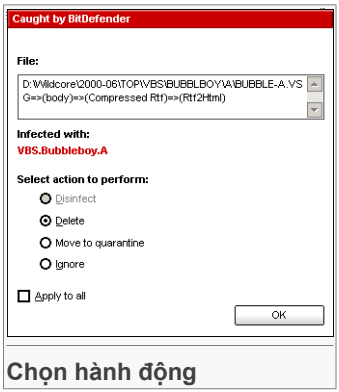
Ghi chú
Quá trình quét có thể mất một lhoảng thời gian, tuỳ thuộc vào độ phức tạp của lần quét.

Ba nút có sẵn:

- **Stop** - mở một cửa sổ mới, từ đó bạn có thể kết thúc quá trình quét. Nhấp vào **Yes&Đóng lại** để thoát khỏi cửa sổ quét.
- **Tạm dừng** - Tạm thời ngưng quá trình quét - bạn có thể tiếp tục bằng cách nhấp vào **Tiếp tục lại**.
- **Cho xem báo cáo** - mở báo cáo quét.

Ghi chú
Nếu bạn nhấp chuột phải vào một nhiệm vụ đang vận hành, một thực đơn tắt (theo bối cảnh) giúp bạn quản lý cửa sổ quét sẽ hiện ra. Các phương án **Tạm dừng / Tiếp tục lại**, **Dừng** và **Stop&Close**)tương tự với các phương án của các nút trong cửa sổ quét.

Nếu phương án **Chỉ dẫn cho Người sử dụng hành động** được đặt trong cửa sổ Các đặc điểm , khi một tập tin nhiễm được phát hiện và một cửa sổ cảnh báo sẽ yêu cầu bạn chọn một hành động để xử lý tập tin bị nhiễm.



Chọn hành động

Bạn có thể xem tên của tập tin và tên của virus.

Chọn một trong các hành động sau để xử lý đối với tập tin bị lây nhiễm:

- **Tẩy rửa** -Tẩy rửa tập tin nhiễm;
- **Xoá** Xoá tập tin nhiễm;
- **Chuyển đến nơi kiểm dịch** - chuyển tập tin bị nhiễm đến nơi kiểm dịch ;
- **Không để ý** - Không để ý đến tập tin bị nhiễm. Không có hành động nào đối với tập tin bị nhiễm.

Nếu bạn quét một thư mục và bạn muốn có hành động giống nhau đối với các tập tin bị nhiễm, chọn hộp kiểm tra tương ứng với **Áp dụng cho tất cả** .

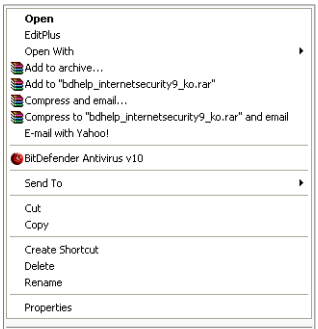
Ghi chú
Nếu phương án **Tẩy trùng** không có hiệu lực, điều đó có nghĩa là tập tin không thể tẩy rửa được. Cách lựa chon tốt nhất là cách ly tập tin đó trong vùng kiểm dịch và gửi nó đến cho chúng tôi phân tích hoặc xoá nó đi.

Nhấp vào **OK**.

Ghi chú
Tập tin báop cáo sẽ được tự động lưu trong phần Scan Logs từ cửa sổ của nhiệm vụ tương ứng **Properties**.

Quét theo bối cảnh

Nhấp chuột phải vào tập tin hoặc thư mục bạn muốn quét và chọn **BitDefender Antivirus v10**.

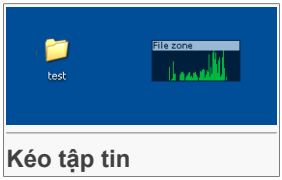


Quét theo bối cảnh

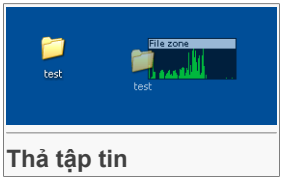
Bạn có thể sửa đổi các phương án quét và xem các tập tin báo cáo bằng cách truy cập vào nhiệm vụ Các đặc điểm cửa sổ của **Quét theo Thực đơn Bối cảnh** .

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

Nếu một tập tin bị nhiễm được phát hiện thì một cửa sổ cảnh báo sẽ xuất hiện yêu cầu bạn chọn một hành động để xử lý đối với tập tin bị nhiễm.

Trong cả hai phương pháp có thể lựa chọn (quét theo bối cảnh và quét kéo & thả, cửa sổ quét sẽ xuất hiện.

7.2.5. Quét các Rootkit

BitDefender sẽ giải quyết các mối hiểm hoạ đối với an ninh mới nhất bằng cách đưa ra một phương tiện phát hiện rootkit cùng với các đầu quét chống gián điệp, virus rất hiệu quả. Bây giờ, BitDefender có kả năng phát hiện các rootkit nằng cách tìm kiểm các tập tin, các thư mục và các quá trình ẩn. Hơn nữa, nó có thểe bảo vệ máy tính của bạn bằng cách đặt tên lại cho các malware sử dụng rootkit.

Để quét máy tính của bạn, tìm các rootkit, hãy vận hành nhiệm vụ **Quét tìm Rootkit**. Một cửa sổ quét sẽ mở ra.

Quan trọng
Khi bạn kiểm tra tìm rootkit, việc rất quan trọng bạn cần phải làm là cài đặt cho BitDefender không được có bất cứ hành động nào đối với các tập tin ẩn.

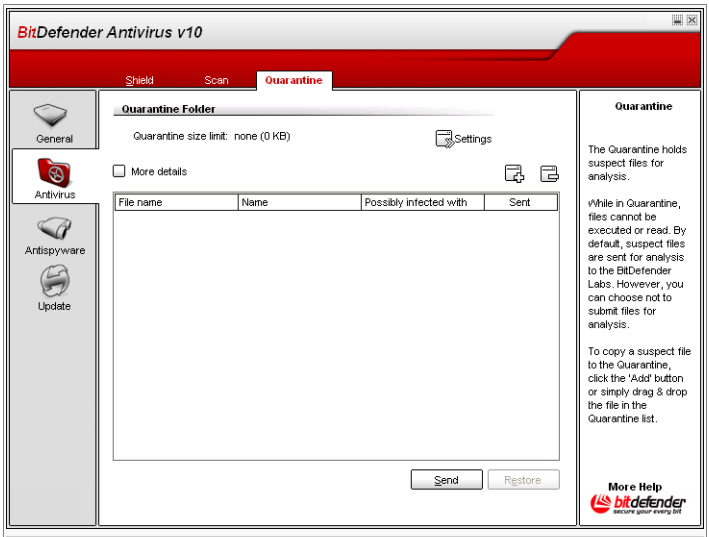
Khi quét xong, bạn có thể thấy kết quả quét.Nếu các tập tin ẩn bị phát hiện, hãy kiểm tra lại cẩn thận: sự hiện diện của các tập tin ẩn có thể biểu thị một khả năng xâm nhập.

Nếu bạn chắc chắn rằng, các tập tin được tìm ra thuộc về malware, chúng tôi khuyến cáo bạn bạn nên cài đặt hành động **Đổi tên các tập tin Rename files** và vận hành lại nhiệm vụ **Quét để tìm Rootkit**. Bằng cách đó, các tập tin ẩn sẽ bị chănk lại.

Cảnh báo
KHÔNG PHẢI TẤT CẢ CÁC TẬP TIN ẨN ĐEEUF LÀ MALWARE! Trước khi đổi tin các tập tin ẩn, cần chắc chắn rằng chúng không thuộc về một ứng dụng đang có hiệu lực mà cũng không thuộc về hệ thống. Đổi tên các tập tin nhe vậy có thể làm cho hệ thống của bạn không sử dụng được.

Quan trọng
Nếu hệ thống của bạn bị hacker quấy phá, chỉ có một cách duy nhất an toàn tránh mọi sự xâm nhập là cài đặt lại hệ thống.

7.3. Kiểm dịch



Kiểm dịch

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

Bộ phận đảm bảo việc quản lý các tập tin được cách ly là **Kiểm dịch**. Module này được thiết kế với chức năng tự động gửi các tập tin bị nhiễm đến phòng thí nghiệm của BitDefender.

Như bạn có thể thấy, phần **Kiểm dịch** chứa một danh sách tất cả các tập tin được cách ly từ trước tới nay. Mỗi một tập tin đều có đính kèm tên, kích cỡ, ngày tháng cách ly và ngày, tháng gửi. Nếu bạn muốn xem thêm thông tin về các tập tin được kiểm dịch, hãy nhấp vào **Thêm Chi tiết** .

Ghi chú
Khi virus được kiểm dịch, 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.

Nhấp vào nút **Add** để bổ sung vào vùng kiểm dịch các tập tin bạn nghi là có bị nhiễm. Một cửa sổ sẽ mở ra và bạn có thể lựa chọn tập tin từ vị trí của nó trên đĩa. Bằng cách này, tập tin sẽ được sao chép lại để kiểm dịch. Nếu bạn muốn chuyển tập

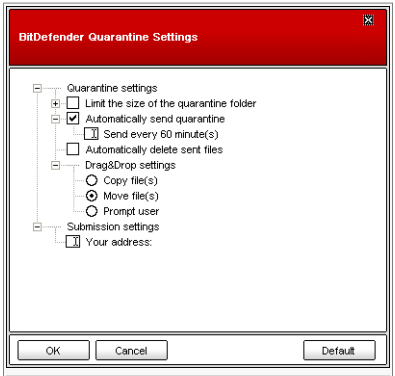
tin đến vùng kiểm dịch, bạn cần phải chọn hộp kiểm tra tương ứng với **Xoá từ vị trí nguyên thuỷ** . Một phương pháp bổ sung nhanh hơn các tập tin bị nghi ngờ vào khu vực kiểm dịch là kéo và thả chúng vào danh mục kiểm dịch.

Để xoá một tập tin được chọn lựa khỏi vùng kiểm dịch, hãy nhấp vào nút **Remove**. Nếu bạn muốn khôi phục lại một tập tin được chọn trở lại vị trí ban đầu của nó thì nhấp vào **Restore**.

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

Quan trọng
Bạn cần phải nêu rõ một số thông tin trước khi bạn có thể gửi các tập tin này đi. Để làm được việc đó, hãy nhấp vào **Settings** và hoàn tất các trường từ phần **Submission settings**, như được miêu tả dưới đây.

Nhấp **Settings** để mở các phương án cao cấp cho vùng kiểm dịch. Cửa sổ sau đấy sẽ được mở ra:



Các phần cài đặt kiểm dịch

Các phương án kiểm dịch được nhóm thành hai phạm trù:

- **Các phần cài đặt kiểm dịch**
- **Các phần cài đặt gửi đi**

Ghi chú
Nhấp vào hộp có "+" để mở một phương án hoặc vào hộp có "-" để đóng một phương án.

Các phần cài đặt kiểm dịch

- **Hạn chế kích thước của thư mục kiểm dịch** - duy trì trong tầm kiểm soát quy mô kiểm dịch. Phương án này được thực hiện bằng cách mặc định và kích thước của nó là 12000 kB. Nếu bạn muốn thay đổi loại giá trị này, hãy đánh một giá trị mới vào trường tương ứng. Nếu bạn chọn hộp kiểm tra tương ứng với **Tự động xoá các tập tin cũ** , khi vùng kiểm dịch đầy, và bạn bổ sung một tập tin mới, các tập tin cũ nhất trong khu vực kiểm dịch sẽ được tự động xoá đi dành chỗ cho các tập tin mới được bổ sung.
- **Gửi cách ly tự động** - tự động gửi những file cách ly tới BitDefender Labs để phân tích. Bạn có thể cài đặt thời gian bằng phút giữa 2 lần gửi liền **Gửi mỗi x phút** field.
- **Tự động xóa các file đã gửi** - tự động xóa các file cách ly sau khi gửi tới BitDefender Lab để phân tích.
- **Drag&Bỏ cài đặt** - nếu bạn dùng phương pháp Drag&Drop và cho file vào cách ly tại đây bạn có thể chọn hành động: copy, chuyển hay hỏi người sử dụng.

Các phần cài đặt kiểm dịch

- **Địa chỉ của bạn** - gõ trong địa chỉ e-mail phòng khi bạn muốn nhận thư mới từ các chuyên gia của chúng tôi,đề cập đến các file không rõ ràng được gửi để phân tích.

Nhấp **Apply** để lưu các thay đổi. Nếu bạn nhấp vào **Default** bạn sẽ tải được các phần cài đặt đã mặc định.

8. Module Chống gián điệp

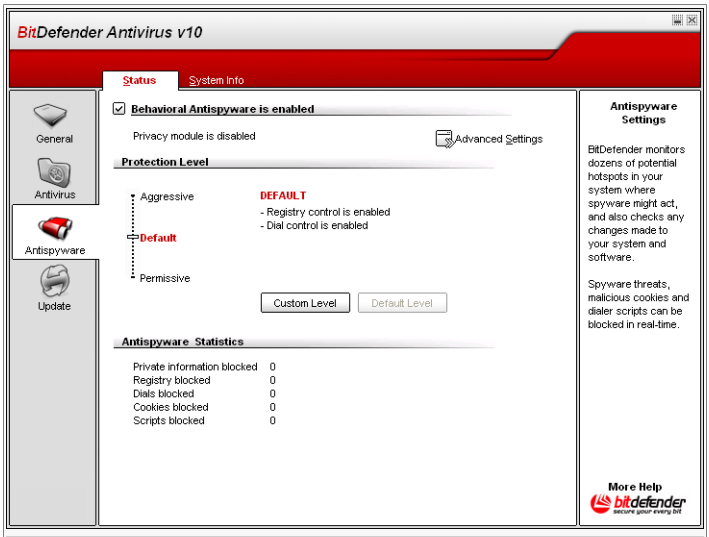
Phần **Chốngvirus** của hướng dẫn sử dụng này chứa đựng các đề tài sau:

- Tình trạng Antispyware
- Cài đặt cấp cao - Kiểm soát riêng tư
- Cài đặt cấp cao-Kiểm soát đăng ký sản phẩm
- Cài đặt cấp cao -kiểm soát quay số
- Cài đặt cấp cao-Kiểm soát cookie
- Cài đặt cấp cao-kiểm soát tập lệnh
- thông tin hệ thống

Ghi chú

Để biết thêm chi tiết về module **Antispyware** xin hãy kiểm tra mô tả về Phần 4.3, "*Module Chống gián điệp*".

8.1. Tình trạng chống gián điệp



Tình trạng chống gián điệp

Trong phần này, bạn có thể hình thành **Antispyware Thái độ**và có thể xem thông tin liên quan đến hoạt động.

Quan trọng
Để ngăn chặn gián điệp lây nhiễm vào máy tính của bạn, hãy giữ cho **Hành vi chống gián điệp**được bảo vệ.

Tại cuối đoạn bạn có thể thấy**Thống kê chống gián điệp**.

Modun**Antispyware** bảo vệ máy tính của bạn khỏi gián điệp thông qua 5 sự 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.
- Kiểm soát Registry - hỏi bạn có cho phép một chương trình thay đổi registry để hoạt động trong Windows start-up.
- Kiểm soát quay điện thoại - hỏi bạn có cho phép một chương trình quay một số điện thoại khi dùng đến modem.

- 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 quét toàn bộ hệ thống chỉ cần nhấp Advanced Settings.

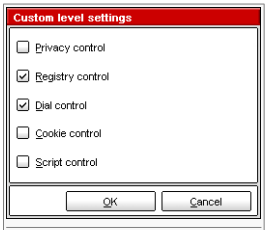
8.1.1. Mức bảo vệ

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 quay điện thoại** và **Kiểm soát riêng tư** đang hoạt động.

Bạn có thể tuỳ chỉnh mức an ninh bằng cách nhấp chuột vào **Mức tự chọn**. cửa sổ sau đây sẽ hiện ra:



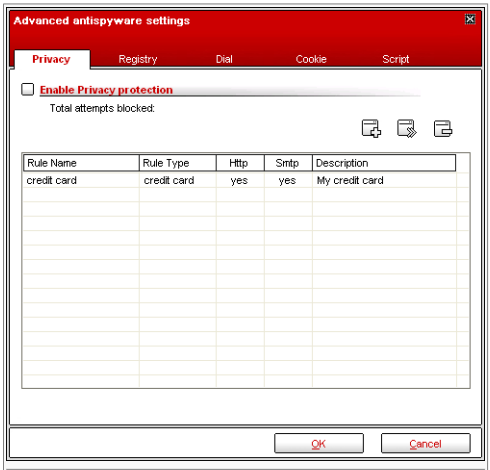
Tuỳ chỉnh mức bảo vệ

Bạn có thể cho phép bất cứ phương án bảo vệ chống gián điệp nào (**Kiểm soát riêng tư**, **Kiểm soát Registry**, **Kiểm soát quay điện thoại**, **Kiểm soát Cookies** and **Kiểm soát Script**).

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

8.2. Cài đặt cấp cao - Kiểm soát riêng tư

Để vào mục này hãy nhấp vào **Cài đặt cấp cao** nút từ modul **Antispyware**, Tình trạng.



Kiểm soát riêng tư

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.

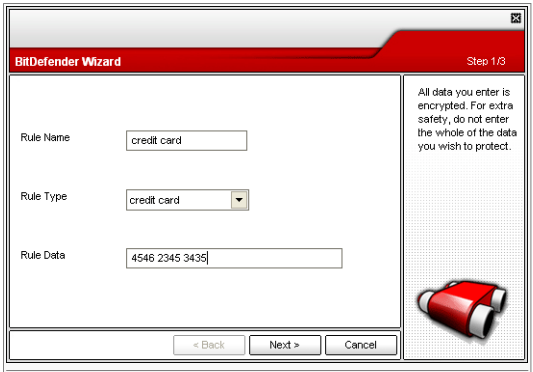
Kiểm soát riêng tư giúp bạn giữ dữ liệu của bạn an toàn. Nó quét những giao dịch HTTP hoặc SMTP, hoặc cả hai, tìm những đoạn viết mà bạn đã định nghĩa. nếu thấy, những trang web hoặc e-mail sẽ bị ngăn chặn.

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.

8.2.1. Thuật sĩ (Wizard) cài đặt

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.

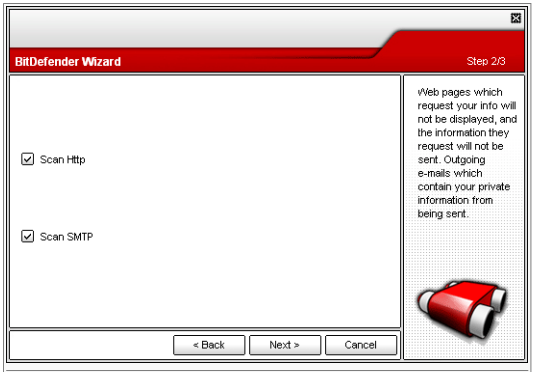
Bạn cần phải cài đặt những thông số sau:

- **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.

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



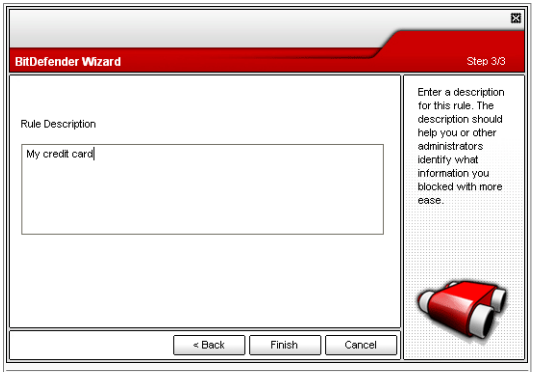
Chọn Giao dịch

Chọn Giao dịch mà bạn muốn BitDefender sẽ quét. Những lựa chọn sau có thể có:

- **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.

Nhấp chuột vào **Next**.

Bước 3/3 - Mô tả Qui tắc



Mô tả Qui tắc

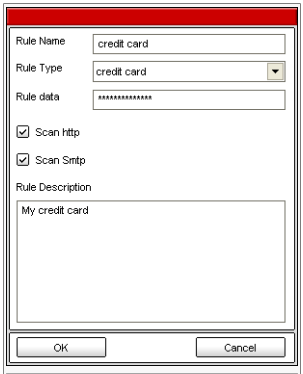
Vào một mô tả ngắn của qui tắc trong trường sửa.

Nhấp vào **Kết thúc**.

bqạn 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:



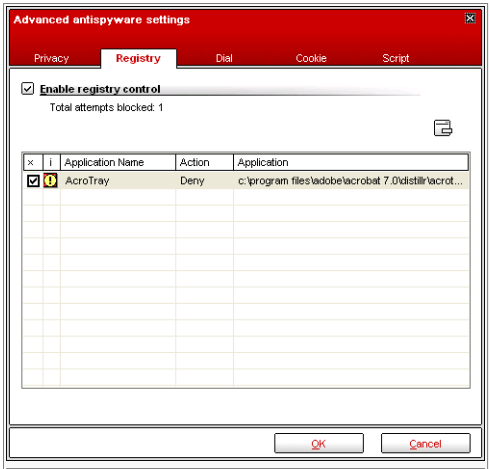
Sửa Qui tắc

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

Để nhập vào mục này hãy vào cửa sổ **cài đặt chống gián cấp cao** (tới modul **Antispyware**, Tình trạng và click **Cài đặt cấp cao**) và click tab **Registry**.



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 câu trả lời**.

Ghi chú
Câu trả lời của bạn sẽ được nhập vào danh sách qui tắc.

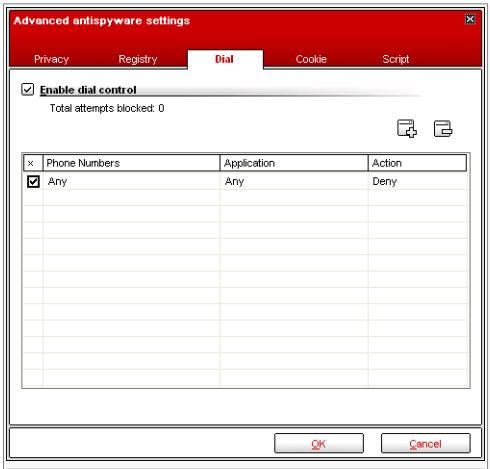
Để xoá phần dứ liệu Registry, hãy chọn nó và nhấp vào nút **Xoá**. Để tạm thời ngừng dữ liệu registry mà không xoá thì chỉ cần bỏ tích tương ứng.

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.

Nhấp **OK**để đóng cửa sổ lại.

8.4. Cài đặt cấp cao - Kiểm soát quay điện thoại

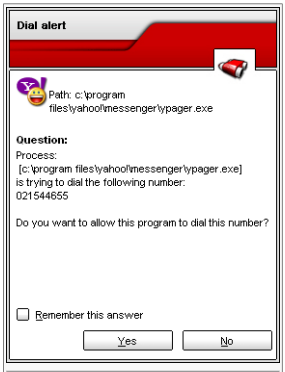
Để thâm nhập vào mục này hãy vào cửa sổ **Advanced Antispyware Settings** (tới modul **Antispyware**, Tình trạng và click **Cài đặt cấp cao**) và click tab **Dial**.



Kiểm soát quay điện thoại

Quay điên thoại (dialer) là một ứng dụng sử dụng modem của máy tính để quay một số điện thoại. Bình thường, những dialer được dùng để quay vào những số có giá tiền cao.

Với **Dial Control** bạn có thể kiểm soát được những số điện thoại nào cho phép hay ngăn chặn. Chức năng này theo dõi tất cả những dialer khi nó muốn đụng đến modem, lập tức người dùng được cảnh báo để cho phép hay ngăn chặn hành động:



Cảnh báo Dial

Bạn có thể xem tên của ứng dụng và số điệnn thoại nó muốn quay.

Tích vào lựa chọn **Nhớ câu trả lời** và click **Yes** hoặc **No** và qui tắc được ghi lại, áp dụng và đưa vào dữ liệu qui tắc. bạn sẽ không bị nhắc lần sau nữa khi quay cùng số đó.

mỗi qui tắc đã được nhớ có thể khởi động trong phần **Dial** mọi lần sau.

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.

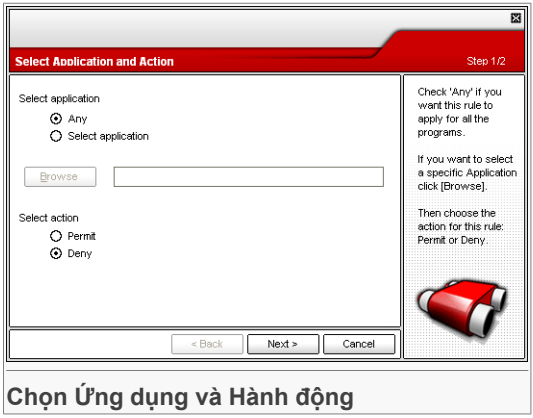
Để xoá một qui tắc, hãy chọn nó và nhấp vào nút **Delete**. Để thay đổi thông số của qui tắc hãy nhấn đúp trường của nó và sửa. Để tạm thời ngừng qui tắc mà không xoá thì chỉ cần bỏ tích.

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 2 bước.

Bước 1/2 - Chọn Ứng dụng và Hành động



Chọn Ứng dụng và Hành động

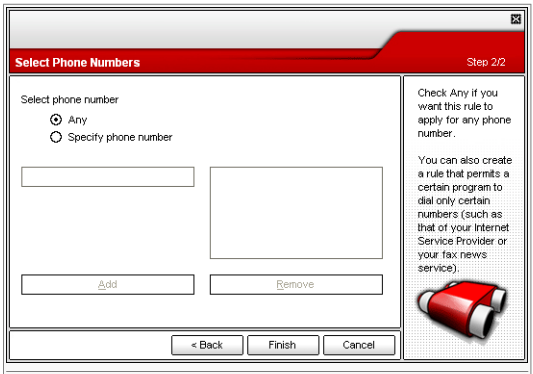
Bạn có thể cài thông số:

- **Ứng dụng** - chọn ứng dụng cho qui tắc. Bạn có thể chỉ chọn ứng dụng (click **Chọn ứng dụng**, sau đó **Browse** và chọn ứng dụng) hoặc tất cả các ứng dụng (ci cần click **Tất cả**).
- **Hành động** - chọn hành động cho qui tắc.

Hành động	Miêu tả
Cho phép	Hành động sẽ được cho phép.
Chặn	Hành độn sẽ bị chặn.

Nhấp chuột vào **Next**.

Bước 2/3 - Chọn Số điện thoại



Chọn Số điện thoại

Click **Chỉ rõ Số điện thoại**, hãy vào số điện thoại mà qui tắc sẽ được áp dụng và click **Thêm**.

Ghi chú
Bạn có thể dùng khi thẻ của bạn trong danh sách số điên thoại cấm của bạn; như 1900* nghiã là những số có bắt đầu bằng 1900 sẽ bị khoá.

Tích **Tất cả** nếu bạn muốn ngăn chặn tất cả các số điện thoại. Để xoá một số nào đó thì chọn và click **Xoá**.

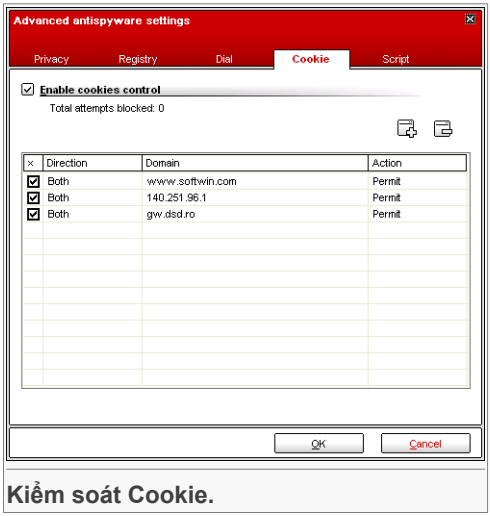
Ghi chú
Bạn có thể đồng thời tạo qui tắc để cho phép một số chương trình để quay những số điện thoại cho sẵn (như số dịch vụ Internet hoặc số Fax mà bạn thường dùng).

Nhấp vào **Kết thúc**.

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

8.5. Cài đặt cấp cao - Kiểm soát cookie

Để vào trong phần này hãy vào cửa sổ **Cài đặt cấp cao Chống Gián điệp** (đi tới phần **Chống Gián điệp** module, Tình trạng và click **Cài đặt cao cấp**) and click the **Cookie**.



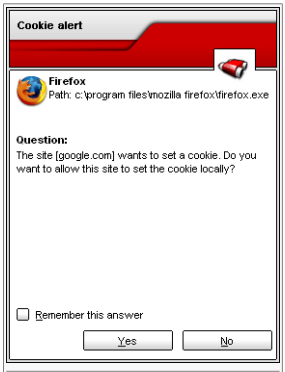
Kiểm soát Cookie.

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.

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.

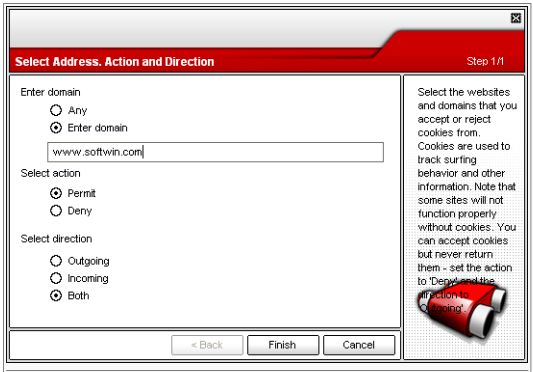
Để xoá một qui tắc, hãy chọn nó và nhấp vào nút **Delete**. Để thay đổi thông số của qui tắc hãy nhấn đúp trường của nó và sửa. Để tạm thời ngừng qui tắc mà không xoá thì chỉ cần bỏ tích.

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, 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.

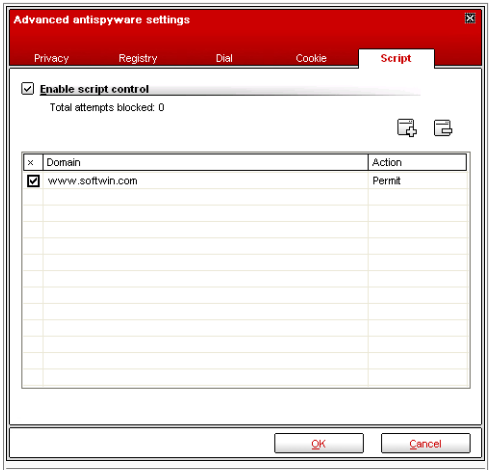
Nhấp vào **Kết thúc**.

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.

8.6. Cài đặt cấp cao - Kiểm soát script

Để vào phần này cần vào cửa sổ **Cài đặt cấp cao chống gián điệp** (vào tab **Antispyware** module, Tình trạng section and click **Cài đặt cấp cao**) và click vào **Script**.

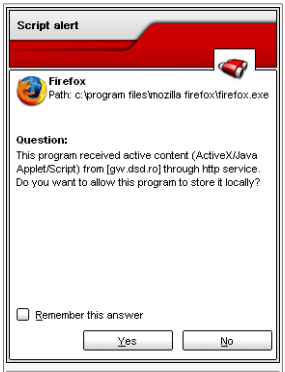


Kiểm soát Script

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.

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.

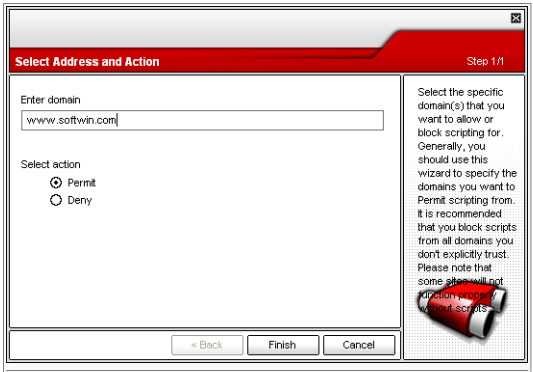
Để xoá một qui tắc, hãy chọn nó và nhấp vào nút **Delete**. Để thay đổi thông số của qui tắc hãy nhấn đúp trường của nó và sửa. Để tạm thời ngừng qui tắc mà không xoá thì chỉ cần bỏ tích.

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.

8.6.1. 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:

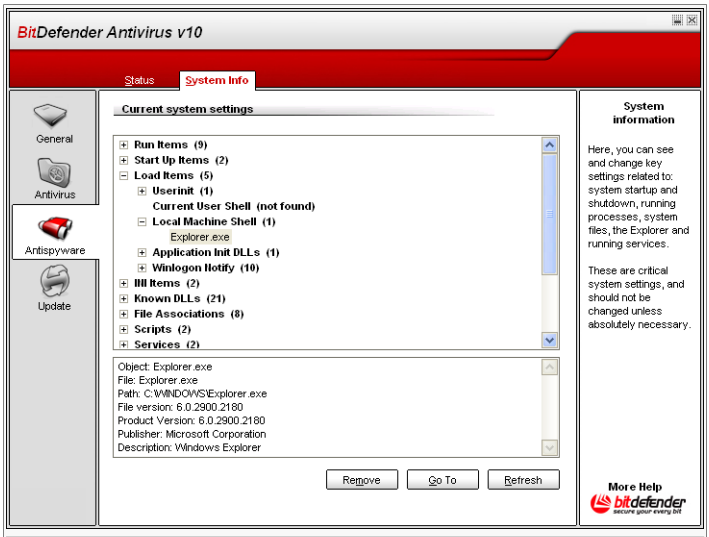
- **Tên Miền** - gõ tên miền để áp dụng vào qui tắc.
- **Hành động** - chọn hành động cho qui tắc.

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.

8.7. Thông tin Hệ thống



Thông tin Hệ thống

Tại đây bạn có thể thay đổi khoá cài đặt thông tin.

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.
- **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**.

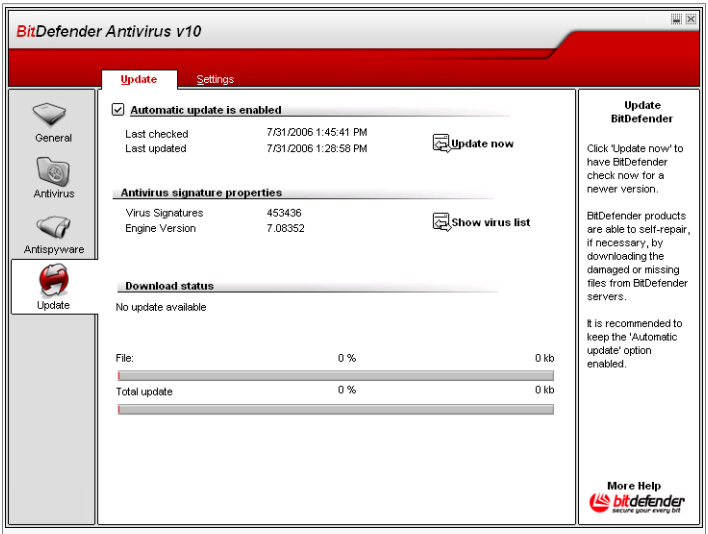
9. Module nâng cấp

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

- Cập nhật Tự động
- Cập nhật Thủ công
- Cài đặt Cập nhật

Ghi chú
Để có thêm chi tiết về module **Cập nhật**, hãy kiểm tra phần miêu tả của "*Module nâng cấp*" (p. 28).

9.1. Cập nhật Tự động



Cập nhật Tự động

Trong phần này, bạn có thể biết về cập nhật - thông tin và thi hành cập nhật.

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

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, từ 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.

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

Modul **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, bạ 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.

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.

9.2. Cập nhật Thủ công

Phương pháp này cài đặt những định nghĩa virus mới nhất. Để cài nâng cấp tới phiên bản cuối cùng, hãy dùng Cập nhật Tự động.

Quan trọng
Chỉ dùng Cập nhật Thủ công khi Cập nhật Tự động không thể hực hiện hoặc khi máy tính của bạn bị gián đợn kết nối Internet.

Có 2 cách để bạn thực hiện việc cập nhật thủ công:

- với file `weekly.exe`;
- với `zip archives`.

9.2.1. cập nhật thủ công với `weekly.exe`

Những gói cập nhật `weekly.exe` được xuất bản vào thứ sáu hàng tuần bao gồm toàn bộ các định nghĩa virus và đông cơ quét nếu có cho đến phiên bản cuối cùng.

Để cập nhật BitDefender dùng `weekly.exe`, hãy tiến hành những bước sau:

1. Download weekly.exe và lưu lại vào trong ổ cứng.
2. Tìm file vừa tài về và nhấn kép chuột vào nó để khởi động cập nhật.
3. Nhấp chuột vào **Next**.
4. Tích **Tôi chấp nhận Thoả thuận Bản quyền** và click **Tiếp**.
5. Click **Install**.
6. Nhấp vào **Kết thúc**.

9.2.2. Cập nhật Thủ công với `zip archives`

Có 2 file lưu trữ zip (archives) trên update server, chứa động cơ quét và chữ ký virus: `cumulative.zip` và `daily.zip`.

- `cumulative.zip` được xuất bản hàng tuần vào thứ hai và nó bao gồm những định nghĩa virus và động cơ quét mới nhất.
- `daily.zip` đuwocj xuất bản hàng ngày bao gồm toàn bộ các cập nhật định nghĩa virus và động cơ quét kể từ khi cập nhật lần cuối.

BitDefender dùng một dịch vụ-kiến trúc cơ sở. Bởi vì đó là thuật pháp để thay thế những định nghĩa virus khác nhau ở những hệ điều hành khác nhau.

- Windows NT-SP6, Windows 2000, Windows XP.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP

Bước tiếp theo:

1. **Tải cập nhật gần nhất.** Nếu là thứ hai, hãy tải từ link cumulative.zip và lưu vào ổ đĩa. Những ngày khác thi tải từ link daily.zip và lưu vào ổ đĩa. nếu đây là lần đầu tiên bạn sử dụng cập nhật thủ công, xin hãy tải cả 2 về.
2. **Dừng bảo vệ BitDefender antivirus.**
   - **Thoát BitDefender management console.** Nhấp chuột phải vào biểu tượng BitDefender từ System Tray và chọn **Thoát**.
   - **Mở dịch vụ.** Bạn click vào **Start**, sau đó **Control Panel**, nhấn kép **Administrative Tools** và click **Services**.
   - **Stop BitDefender Virus Shield service.** Chọn dịch vụ **BitDefender Virus Shield** trong danh sách và click **Stop**.

- **Stop BitDefender Scan Server service.** Chọn dịch vụ **BitDefender Scan Server** trong danh sách và click **Stop**.

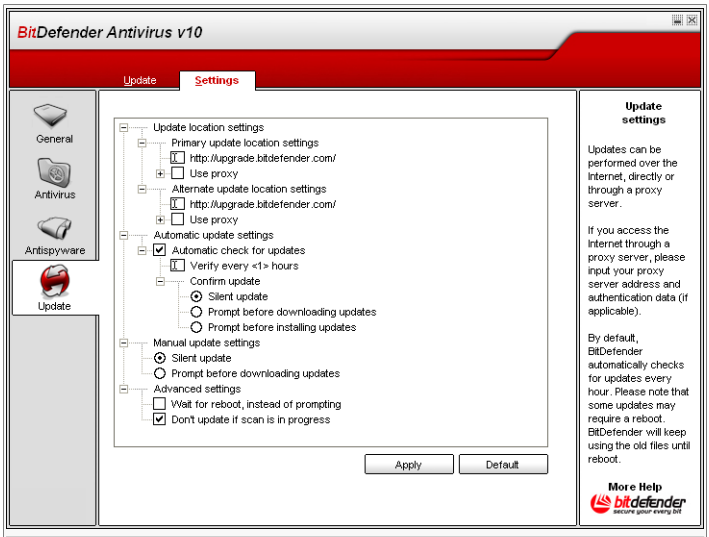
3. **Giải nén.** Khởi động `cumulative.zip` khi cả hai file lưu trữ đều có. Giải nén vào trong thư mục `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` và chấp nhận ghi đè.
4. **Khởi động lại BitDefender antivirus.**
   - **Khởi động dịch vụ BitDefender Scan Server.** Chọn dịch vụ **BitDefender Scan Server** từ trong danh sách và click **Start**.
   - **Khởi động dịch vụ BitDefender Virus Shield.** Chọn dịch vụ **BitDefender Virus Shield** từ trong danh sách và click **Start**.
   - **Mở BitDefender management console.**

Windows 98, Windows Millennium

Bước tiếp theo:

1. **Tải cập nhật gần nhất.** Nếu là thứ hai, hãy tải từ link cumulative.zip và lưu vào ổ đĩa. Những ngày khác thi tải từ link daily.zip và lưu vào ổ đĩa. nếu đây là lần đầu tiên bạn sử dụng cập nhật thủ công, xin hãy tải cả 2 về.
2. **Giải nén.** Khởi động `cumulative.zip` khi cả hai file lưu trữ đều có. Giải nén vào trong thư mục `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` và chấp nhận ghi đè.
3. **Khởi động lại máy tính.**

9.3. Cài đặt cập nhật



Cài đặt cập nhật

Ccó thể cập nhật từ một máy của mạng LAN, thông qua Internet, trực tiếp hoặc qua proxy server.

Cử sổ có bốn phạm trù phương án cập nhật (**Cài đặt cập nhật nội bộ**, **Lựa chọn cập nhật tự động**, **Cài đặt cập nhật thủ công** và **Lựa chọn cấp cao**) tổ chức trong một menu, giống như trong Windows.

Ghi chú
Nhấp vào hộp có "+" để mở một phương án hoặc vào hộp có "-" để đóng một phương án.

9.3.1. Cài đặt Cập nhật Nội bộ

Để cập nhật nhanh hơn và hiệu quả hơn, bạn có thể cài đặt 2 điểm cập nhật: **Điểm cập nhật đầu** và **Điểm cập nhật thay thế**. Bạn đề phải cài đặt những lựa chọn sau cho cả 2:

- **Điểm cập nhật** - Nếu bạn nối với mạng nội bộ mà có một máy có cập nhật chủ của BitDefender, bạn có thể chỉ cho máy cập nhật qua đó. Mặc định là: http://upgrade.bitdefender.com.

- **Dùng proxy** - Nếu công ty bạn dùng proxy server hãy xem lại lựa chọn này. Bạn cần phải cài đặt như sau:
  - **Proxy sets** - Gõ IP hoặc tên của proxy server và cổng dùng cho BitDefender để nối với proxy server.

    Quan trọng
    Syntax: `name:port` or `ip:port`.

  - **Proxy user** - hãy vào tên người sử dụng mà proxy nhận biết được.

    Quan trọng
    Syntax: `domain\user`.

  - **Proxy password** - hãy vào mật khẩu đúng của người dùng.

9.3.2. Lựa chọn Cập nhật Tự động

- **Tự động tìm cập nhật** - BitDefender tự động tìm dịch vụ để cập nhật cho bạn.
- **Kiểm tra từng x giờ** - Thiết lập nhịp độ BitDefender tìm cập nhật. Mặc định là 1 giờ.
- **Cập nhật im lặng** - BitDefender tự động tải và cài đặt cập nhật.
- **Hỏi trước khi tải** - mỗi khi có bản cập nhật bạn sẽ được hỏi trước khi tải.
- **Hỏi trước khi cài** - sau mỗi khi tải bản cập nhật về bạn sẽ được hỏi trước khi cài.

Quan trọng
Nếu bạn chọn **Hỏi trước khi tải** hoặc **Hỏi trước khi cài** và bạn đóng&thoát thanh quản lý cập nhật tự động sẽ không thực hiện.

9.3.3. Quản lý Cài đặt Thủ công

- **Cập nhật im lặng** - cập nhật thủ công sẽ được thực hiện tự động đằng sau.
- **Hỏi trước khi tải** - mỗi khi bạn muốn cập nhậtn thủ công bạn sẽ được hỏi lại trước khi tải và cài đặt cập nhật.

Quan trọng
Nếu bạn chọn **Hỏi trước khi tải** và bạn đóng&thoát thanh quản lý cập nhật thủ công sẽ không được thực hiện.

9.3.4. Lựa chọn cấp 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.

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

Các thực hành tốt nhất

10. Các thực hành tốt nhất

Phần **Nên làm nhất** của cẩm nang người sử dụng này chứa các đề tài sau:

- Làm thế nào để bảo vệ máy tính chống mối đe doạ tin tặc
- Cài đặt công việc quét như thế nào

10.1. Làm thế nào để bảo vệ máy tính chống mối đe doạ tin tặc

Hãy theo những bước sau để bảo vệ máy tính của bạn chống virus, gián điệp và những phần mềm xấu:

1. **Kết thúc thuật sĩ cài đặt đầu tiên.** Trong quá trình cài đặt sẽ có một wizard xuất hiện. Thuật sĩ (wizard) này giúp bạn đăng ký **BitDefender Antivirus v10**, tạo ra một tài khoản BitDefender và lắp đặt BitDefender để thực hiện các nhiệm vụ an ninh quan trọng.

   Quan trọng
   Nếu bạn có BitDefender Rescue CD, hãy quét máy tính của bạn trước khi cài BitDefender để biết được máy tính của bạn có phần mềm phá hoại hay không.

2. **Cập nhật BitDefender.** Nếu bạn chưa hoàn thành thuật sĩ cài đặt đầu tiên, hãy cập nhật theo yêu cầu (tới modul **Cập nhật**, Cập nhật và click **Cập nhật Ngay**).
3. **Quét toàn bộ hệ thống.** Vào phần **Antivirus** module, Shield và click **Quét Ngay**.

   Ghi chú
   Bạn có thể khởi đầu quét toàn hệ thống từ phần Quét. Chọn nhiệm vụ **Quét toàn hệ thống** và click **Chạy nhiệm vụ**.

4. **Ngăn ngừa nhiễm.** Trong phần **Lá chắn**, giữ Bảo vệ tức thì bật để bảo vệ bạn chống virus, gián điệp và những phần mềm xấu. Thiết lập mức bảo vệ phù hợp với yêu cầu nhất. Bạn có thể tuỳ chọn bất cứ lúc nào bạn muốn bằng cách nhấn **Mức tuỳ chọn**.

   Quan trọng
   Đặt trình cho BitDefender Antivirus v10 để quét cả hệ thống của bạn ít nhất một tuần một lần bằng cách đặt lịch nhiệm vụ **Quét Toàn Hệ thống** từ phần Quét.

5. **Hãy giữ cho BitDefender luôn hiện.** Trong phần modul **Cập nhật**, phần Cập nhật hãy giữ cho **Cập nhật Tự động** kích hoạt để bảo vệ hệ thống chống lại những mối đe doạ mới nhất.
6. **Lập lịch quét toàn bộ hệ thống.** Tới phần **Quét** và chương trình BitDefender để quét hệ thống của bạn ít nhất mỗi tuần một lần bằng cách lên lịch cho nhiệm vụ **Quét toàn hệ thống**.

10.2. Cấu hình cho Nhiệm vụ quét như thế nào

Hãy theo các bước sau để lập và cấu hình cho một nhiệm vụ quét:

1. **Thiết lập nhiệm vụ mới.** Tới phần Quét và nhấp vào **Nhiệm vụ mới**. Cửa sổ Đặc điểmsẽ xuất hiện.

Ghi chú
Bạn cũng có thể thiết lập một nhiệm vụ mới bằng cách sao chép lại một nhiệm vụ đã có sẵn. Để làm được điều này, nhấp chuột phải vào một nhiệm vụ và chọn **Sao lại** từ thực đơn tắt. Nhấp đúp vào sao lại (duplicate) để mở cửa sổ **Đặc điểm**.

2. **Đặt mức độ quét.** Tới phần **Tổng quan** để cài mức độ quét. Nếu bạn muốn, bạn có thể tuỳ biến các phần cài đặt bằng cách nhấp chuột vào **Tuỳ chọn**.
3. **Cài mục tiêu quét.** Đi tới phần **Đường Quét** và chọn các mục tiêu bạn muốn quét.
4. **Lên lịch quét.** Nếu nhiệm vụ quét phức tạp, bạn có thể phải lên lịch cho nó ở giai đoạn sau khi máy của bạn đang ở trong tình trạng nhàn rỗi. Điều này sẽ giúp BitDefender hoàn thành một nhiệm vụ quét chính xác hệ thống của bạn. Tới phần **Lên Lịch** đến Lên lịch cho nhiệm vụ .

Đĩa CD Hồi phục BitDfender

BitDefender Antivirus v10 đi cùng với một đĩa CD có thể khởi động được (Đĩa CD cứu giúp được duaj 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), các phần dùng chung Samba/Windows từ xa hoặc các điểm cài đặt NFS. Một giao diện cấu hình dựa trên web cho các giải pháp của BitDefender cũng được đưa vào.

11. Tổng quan

Các tính năng nóng

- Bảo vệ nhanh email (Chống virus & Chống thư rác)
- Các giải pháp chống Virus cho ổ cứng của bạn
- Hỗ trợ viết NTFS (Sử dụng Captive project)
- Tẩy rửa các tập tin bị nhiễm trong các phần của Windows XP

11.1. KNOPPIX là gì?

Trích dẫn từ http://knopper.net/knoppix:

“ KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. ”

11.2. 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

Trị số tối thiểu được chấp nhận là 64MB, khuyến cáo nên dung loại 128MB để có hoạt động tốt hơn.

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

Độ phân giải đồ hoạ được khuyến cáo thấp nhất là 800x600 cho công tác quản lý dựa trên web.

11.3. Phần mềm được đưa vào

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

- BitDefender SMTP Proxy (Chống thư rác & Chống virus)
- Quản lý BitDefender từ xa (cấu hình dựa trên web)
- Ấn bản BitDefender Linux (máy quét virus) + Giao diện GTK
- Tư liệu BitDefender (PDF & HTML format)
- Các phần thêm của BitDefender (Artwork, Leaflets)
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS – Hệ thống Tập tin File System
- Các công cụ phục hồi dữ liệu và sửa chữa hệ thống, thậm chí là cho cả các hệ thống đang hoạt động khác
- Network và các công cụ phân tích an ninh cho các nhân viên quản trị network
- Giải pháp sao chép dự phòng Amanda
- thttpd
- Phân tích lưu lượng mạng Ethereal, Màn hình IPTraf IP LAN
- Kiểm định an ninh mạng Nessus
- Parted, QTParted and partimage, partition resize, save & Giải pháp phục hồi
- Adobe Acrobat Reader
- Mozilla Firefox Web browser

11.4. BitDefender Linux Security Solutions

Đĩa CDLinuxDefender bao gồm BitDefender SMTP Proxy Chống virus/Chống thư rác cho Linux, Quản trị BitDefender từ xa (Một giao diện trên trang web-based để cấu hình máy quét theo yêu cầu BitDefender SMTP Proxy) và BitDefender Linux Edition.

11.4.1. BitDefender SMTP Proxy

BitDefender cho Linux Mail Servers - SMTP Proxy là một giải phảp kiểm tra, tiến hành bảo vệ chống virus và thư rác ở cấp cổng vào bằng cách quét tất cả các lưu lượng thư từ để tìm các malware đã được biết tới hoặc chưa được biết tới. Là kết quả của một công nghệ độc quyền và độc đáo, BitDefender dành cho các Mail Server tương

thích với đại đa số các nền thư điện từ hiện hành và được cấp chứng chỉ "RedHat Ready".

Giải pháp chống thư rác và chống virus này quét, tẩy rửa và lọc lưu lượng thư điện tử cho bất cứ loại server thư từ hiện hành nào, bất kể nền và hệ thống vận hành. BitDefender SMTP Proxy được vận hành vào thời gian khởi động và quét tất cả các lưu lượng thư từ đến và đi. Để cấu hình cho BitDefender SMTP Proxy, Sử dụng Quản trị Từ xa BitDefender theo các chỉ dẫn dưới đây.

11.4.2. Quản trị Từ xa BitDefender BitDefender Remote Admin

Bạn có thể cấu hình và quản lý các dịch vụ của BitDefender từ xa hoặc cục bộ (Sau khi bạn đã cấu hình mạng của bạn) bằng cách theo các bước sau:

1. Khởi động Firefox browser và tải BitDefender Remote Admin URL: https://localhost:8139 (hoặc nhấp đúp vào biểu tượng BitDefender Remote Admin trên màn hình của bạn)
2. Log in với "bd" người sử dụng và "bd" mật mã
3. Chọn "SMTP Proxy" trên thực đơn phía bên trái
4. Cài đặt Real SMTP server và cổng nghe
5. Thêm các vùng email vào bộ tiếp sóng
6. Thêm các vùng mạng vào bộ tiếp sóng
7. Chọn "Chống thư rác " trên thực đơn bên trái để cáu hình các khả năng chống thư rác
8. Chọn "Chống Virus" để cấu hình các hành động chống virus của BitDefender (Làm gì khi phát hiện ra virus, nơi kiểm dịch)
9. Thêm vào đó, bạn có thể cấu hình "Các thông báo thư từ " và khả năng ghi chép ("Logger")

11.4.3. Ấn bản BitDefender Linux

Bộ phận quét virus trong LinuxDefender được đưa thẳng vào màn hình của bạn. Phiên bản này mô tả những nét nổi bật của GTK+ giao diện đồ hoạ.

Chỉ cần lướt qua đĩa cứng của bạn (hoặc các phần dùng chung được cài đặt sẵn), nhấp chuột phải vào bất cứ tập tin hoặc thư mục nào và chọn "Quét b BitDefender". Ấn bản BitDefender Linux sẽ quét những danh mục được chọn và hiển thị báo cáo tình hình. Để biết các phương án chi tiết,hãy xem tư liệu của Ấn phẩm BitDefender Linux Edition (Trong thư mục tư liệu của BitDefender hoặc trang cẩm nang) và chương trình **/opt/BitDefender/lib/bdc**.

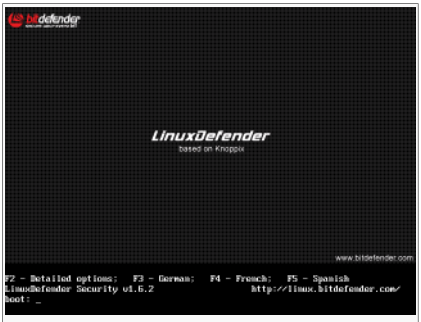
12. LinuxDefender Howto

12.1. Khởi động và dừng lại

12.1.1. Khởi động LinuxDefender

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.

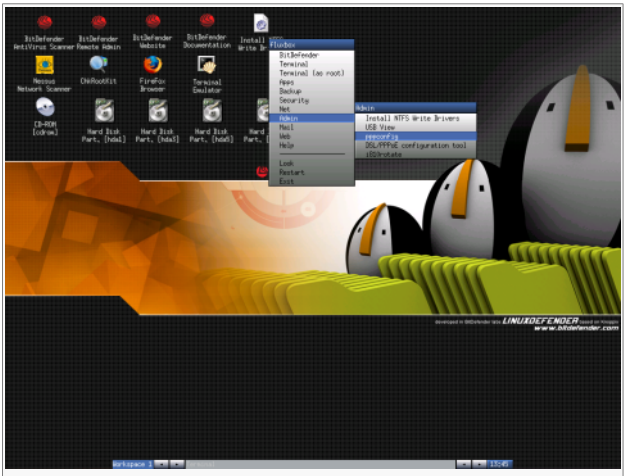
Chờ cho đến khi màn hình tiếp theo xuất hiện và theo các chỉ dẫn trên màn hình để khởi động LinuxDefender.



Khởi động màn hình Splash

Nhấn F2 để có các phương án chi tiết. Nhấn F3 để có các phương án chi tiết bằng tiếng Đức. Nhấn F4 để có các phương án chi tiết bằng tiếng Pháp. Nhấn F5 để có các phương án chi tiết bằng tiếng Tây Ban Nha. Để khởi động nhanh với các phương án mặc định chỉ cần nhấn vào ENTER.

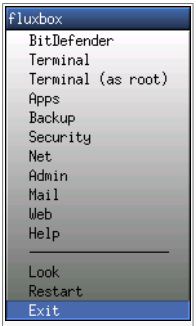
Khi quá trình khởi động kết thúc, bạn sẽ nhìn thấy màn hình nền tiếp theo. Bây giờ bạn có thể sử dụng LinuxDefender.



Màn hình nền

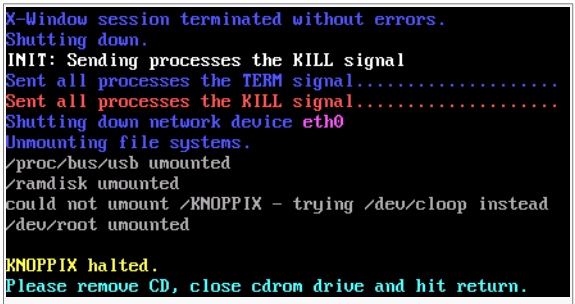
12.1.2. Dừng LinuxDefender

Để thoát đúng cách khỏi LinuxDefender, chúng tôi khuyến cáo bạn nên lấy tất cả các phần đã được đưa vào bằng cách sử dụng lệnh **umount** hoặc bằng cách nhấp chuột phải vào các biểu tượng riêng trên màn hình nền và chọn **Unmount**. Sau đó 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 When 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

12.2. Cấu hình nối mạng Internet

Nếu bạn đang ở mạng DHCP và bạn có một card mạng Ethernet network card, việc nối mạng Internet sẽ phải được phát hiện và cấu hình xong. Để có cấu hình cẩm nang, hãy theo các bước tiếp theo.

1. Mở thực đơn LinuxDefender (nhấp chuột phải) và chọn **Terminal** để mở một console.
2. Đánh **netcardconfig** vào terminal mở để khởi động công cụ cấu hình mạng.
3. Nếu mạng của bạn đang sử dụng DHCP, hãy chọn **yes** (Nếu bạn không chắc chắn, hãy hỏi nhân viên quản trị mạng). Nếu không, mời bạn xem phần dưới đây.
4. Việc nối mạng sẽ phải được cấu hình bây giờ. Bạn có thể thấy IP của bạn và các phần cài đặt card mạng với lệnh **ifconfig**.
5. Nếu bạn có một IP tĩnh (bạn không sử dụng DHCP), hãy chọn **No** trong câu hỏi DHCP.
6. Hãy theo các chỉ dẫn trên màn hình. Nếu bạn không chắc chắn phải viết những gì, hãy liên hệ với hệ thống của bạn hoặc nhân viên quản trị mạng để biết thêm chi tiết.

Nếu mọi công đoạn đều trôi chảy, bạn có thể thử nghiệm việc nối mạng của bạn bằng "ping-ing" `bitdefender.com`.

```
$ ping -c 3 bitdefender.com
```

Nếu bạn sử dụng cách nối mạng quay số, hãy chọn **pppconfig** từ LinuxDefender / thực đơn Quản trị Admin menu. Sau đó, theo các chỉ dẫn trên màn hình để cài đặt một kết nối Internet PPP.

12.3. Cập nhật BitDefender

Các gói của BitDefender cho LinuxDefender sử dụng đĩa ảo (ramdisk) của hệ thống cho các tập tin có thể cập nhật được. Bằng cách này, bạn có thể cập nhật tất cả các chữ ký virus các đầu quét và các cơ sở dữ liệu chống thư rác, thậm chí nếu như bạn vận hành hệ thống từ các phương tiện read-only media như một CD LinuxDefender.

Hãy chắc chắn rằng bạn đang nối mạng Internet. Đầu tiên hãy mở Quản trị BitDefender Từ xa và chọn **Live! Update** từ thực đơn phía bên trái. Nhấn **Cập nhật bây giờ** để kiểm tra các danh mục mới được cập nhật.

Lần lượt, bạn có thể phát lệnh sau trong một terminal.

```
# /opt/BitDefender/bin/bd update
```

Tất cả các quá trình cập nhật sẽ được ghi vào sổ ghi chép đã được mặc định của BitDefender. Bạn có thể xem bằng lệnh tiếp theo.

```
# tail -f /ramdisk/BitDefender/var/log/bd.log
```

Nếu bạn sử dụng một proxy cho các kết nối ngoại vi, hãy cấu hình các phần cài đặt Proxy settings trong **Live! Cập nhật** thực đơn, **Configuration** tab.

12.4. Quét Virus

12.4.1. Tôi truy cập các dữ liệu Windows của mình như thế nào ?

Hỗ trợ ghi NTF

Hỗ trợ viết NTFS có sẵn, sử dụng Captive NTFS write project. Bạn cần hai tập tin điều khiển từ phần cài đặt Windows của bạn: `ntoskrnl.exe` and `ntfs.sys`. Hiện tại, chỉ có các phần điều khiển của Windows XP được hỗ trợ. Chú ý là bạn cũng có thể sử dụng chúng để truy cập các phần của Windows 2000/NT/2003.

Lắp đặt các bộ phận điều khiển NTFS

Để truy cập các phần NTFS Windows của bạn và để có thể viết các dữ liệu lên đó, trước tiên, bạn cần phải cài đặt các bộ phận điều khiển. Nếu bạn không sử dụng NTFS cho các phần Windows mà sử dụng FAT, hoặc bạn chỉ cần truy cập dữ liệu để

đọc, bạn có thể đưa trực tiếp đĩa vào và truy cập các đĩa của Windows giống như bất cứ đĩa nào của Linux.

Để trợ giúp têm cho các phần NTFS, trước tien bạn cần phải cài đặt các đĩa NTFS từ các ổ đĩa cứng của bạn, từ các phần dung chung từ xa, từ USB hoặc từ phần Nâng cấp của Windows Update. Chúng tôi khuyến cáo bạn nên sử dụng các ổ đĩa từ một vùng được biết chắc là an toàn bởi vì các ổ đĩa cục bộ từ máy chủ của Windows có thể bị nhiễm virus hoặc bị hư hỏng.

Nhấp đúp **Cài đặt các đầu ghi NTFS** biểu tượng trên màn hình nền để vận hành **BitDefender Captive NTFS Installer**. Chọn giải pháp thứ nhất nếu bạn muốn cài đặt các ổ đĩa từ ổ đĩa cứng cục bộ.

If the drivers are in a common location, use **Quick search** to find the drivers."*m*s*gstr “Tất cả các lựa chọn sản phẩm được in sử dụng các ký tự **mạnh**.

Lần lượt, bạn có thể nêu cụ thể cácc ổ đĩa của bạn được tìm thấy ở đâu. Hoặc bạn có thể tải các ổ đĩa từ Windows Update SP1.

Các ổ đĩa chưa được cài đặt trên ổ cứng nhưng được LinuxDefender sử dụng tạm thời để truy cập các phần của Windows NTFS. Nếu chương trình cài đặt các ổ đĩa NTFS, bạn có thể nhấp đúp vào các biểu tượng trên màn hình nền các phần của NTFS và duyệt qua nội dung. Để tăng cường quản lý tập tin, hãy sử dụng Midnight Commander từ thực đơn LinuxDefender (hoặc đánh **mc** vào một console).

12.4.2. Làm cách nào để quét virus?

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.

```
# /opt/BitDefender/bin/bdgtk2/path/to/scan/
```

Sau đó nhấp vào **Bắt đầu quét**.

Nếu bạn muốn cấu hình các phương án chống virus, hãy chọn **Cấu hình chống virus** tab từ bảng bên trái của chương trình.

12.5. Thiết lập một Toaster lọc nhanh các thư tín.

Bạn có thể sử dụng LinuxDefender để tạo ra một phương án lọc thư từ đặc biệt mà không cần phải cài đặt bất cứ một phần mềm nào cũng như không cần phải sửa đổi mail server. Ý tưởng ngầm ở đây là đặt một hệ thống LinuxDefender ngay trước mail server của bạn, cho phép BitDefender quét tìm thư rác và virus trong tất cả lưu lượng SMTP và đặt lại nó vào mail server thật.

12.5.1. Các điều kiện tiên quyết

Bạn sẽ cần phải có một PC với Pentium 3 compatible CPU hoặc mới hơn, ít nhất là 256MB RAM và một đĩa CD/DVD để khởi động từ đó. Hệ thống LinuxDefender sẽ phải nhận lưu lượng SMTP thay vì mail server thật. Có một số cách để cài đặt nó.

1. Đổi IP của mail server thật của bạn và ấn định IP cũ cho hệ thống LinuxDefender
2. Đổi các bản ghi DNS sao cho mục vào MX cho các miền của bạn nhằm vào hệ thống LinuxDefender
3. Cài đặt các trang chủ email của bạn để sử dụng hệ thống LinuxDefender mới như máy chủ SMTP.
4. Thay đổi các phần cài đặt tường lửa để tiếp tới / chuyển hướng tất cả các kết nối SMTP tới hệ thống LinuxDefender thay vì đến máy chủ email thật

LinuxDefender howto sẽ không giải thích bất cứ điều gì liên quan đến các vấn đề trên. Để biết thêm chi tiết, bạn có thể tham khảo Các hướng dẫn cho mạng Linux and Tư liệu Netfilter.

12.5.2. The email toaster

Khởi động CD LinuxDefender và chờ cho đến khi hệ thống X Windows được tải và hoạt động.

Để cấu hình BitDefender SMTP Proxy, nhấp đúp vào biểu tượng trên màn hình nền **Quản trị BitDefender Từ xa** . Cửa sổ sau đây sẽ xuất hiện. Sử dụng `bd` tên người sử dụng và `bd`àmatj mã để đăng nhập vào Quản trị BitDefender Từ xa.

Sau khi đăng nhập thành công, bạn sẽ có thể cấu hình cho BitDefender SMTP Proxy.

Chọn**SMTP Proxy** để cấu hình máy chủ email thật mà bạn muốn bảo vệ chống thư rác và virus.

Chọn **Các miền Email** tab để vào tất cả các miền mà bạn muốn chấp nhận email.

Nhấn vào **Thêm miền Email** hoặc **Thêm các miền thư tín hàng loạt** và theo các chỉ dẫn trên màn hình để cài các miền email.

Chọn **Các miền Net** tab để vào tất cả các mạng mà bạn muốn đặt lại email vào.

Nhấn **Thêm Miền Net** hoặc **Thêm các miền Net thư tín hàng loạt** và theo các chỉ dẫn trên màn hình để cài đặt các miền mạng relay.

Chọn **Chống virus** từ thực đơn bên trái để chọn phải làm gì khi phát hiện ra virus và để cấu hình các phương án chống virus khác.

Bây giờ tất cả các lưu lượng SMTP được quét và lọc bởi BitDefender.Bằng mặc định, tất cả các thông điệp bị nhiễm virus đã được tẩy rửa hoặc bỏ đi và tất cả các thư rác bị BitDefender phát hiện được gom lại vào một chủ đề với cái tên `[SPAM]`. Một đầu đề email (`X-BitDefender-Spam: Yes/No`) được bổ sung cho tất cả các email để làm bớt công việc lọc thư cho phía đối tác.

12.6. Thực hiện kiểm định an ninhh Mạng

Ngoài các khả năng chống malware, khôi phục dữ liệu và lọc thư tín, LinuxDefender còn có một bộ các công cụ thực hiện công tác kiểm định an ninh mạng host & Kiểm định an ninh mạng. Việc phân tích mang tính pháp lý các hệ thống bị tổn thương cũng có thể tiến hành được bằng việc sử dụng các phương tiện an ninh gắn kèm với LinuxDefender. Đọc chỉ dẫn nhỏ sau để biết làm thế nào bạn có thể bắt đầu một cuộc kiểm định an ninh nhỏ cho các máy chủ và các mạng công tác của bạn.

12.6.1. Kiểm tra tìm các Rootkit

Trước khi bắt đầu tìm kiếm các vấn đề an ninh trên các máy tính nối mạng, trước tiên, bạn phải chắc chắn rằng, máy chủ LinuxDefender không bị hư hại.Bạn có thể thực hiện việc quét virus cho các ổ cứng đã được cài đặt như được nêu trong hướng dẫn **Quét tìm virus** hoặc bạn có thể quét các Unix rootkit.

Trước tiên hãy cài tất cả các phần của ổ đĩa cứng, nhấp đúp vào các biểu tượng của chúng trên màn hình hoặc bằng cách sử dụng lệnh **mount** trong console. Sau đó nhấp đúp vào biểu tượng **Kiểm tra RootKit** để kiểm tra nội dung của CD hoặc khởi động lệnh **chkrootkit** trong console, sử dụng `-r NEWROOT` thông số để xác định cụ thể thư mục mới /(gốc) của máy chủ.

```
# chkrootkit -r /dev/hda3
```

Nếu tìm thấy một rootkit, chkrootkit sẽ hiển thị phát hiện này trong **BOLD**, sử dụng chữ viết hoa.

12.6.2. Nessus – Máy quét mạng

Nessus là một máy quét cho những điểm yếu, nó là một chương trình mở, thông dụng nhất trên thế giới và được trên 75.000 tổ chức trên thế

> giới sử dụng. Nhiều tổ chức lớn nhất trên thế giới đã tiết kiệm được đáng kể các chi phí nhờ sử dụng Nessus để kiểm tra các thiết bị và các ứng dụng quan trọng trong doanh nghiệp.
>
> *—www.nessus.org*

Nessus có thể được sử dụng để quét từ xa các máy tính trong mạng của bạn, chống lại rất nhiều các nguy cơ gây thương tổn cho máy tính và hệ thống. Một số biện pháp được khuyến cáo phải tiến hành để làm giảm nhẹ các nguy cơ liên quan đến an ninh và ngăn ngừa các sự cố an ninh.

Nhấp đúp vào biểu tượng trên màn hình **Máy quét An ninh** hoặc vận hành **startnessus** từ một terminal. Đợi cho đến khi cửa sổ sau xuất hiện. Tuỳ thuộc vào các tài nguyên trong phần cứng của bạn, có thể phải mất tới 10 phút để tải Nessus cùng với trên 5000 plugins chứa các cơ sở dữ liệu có thể bị tổn thương. Sử dụng `knoppix` người sử dụng và `knoppix` mật mã để đăng nhập.

Nhấp chuột vào **Chọn tab mục tiêu** tab và enter IP của máy tính hoặc tên của máy chủ mà bạn muốn quét để xử lý các vị trí có khả năng bị tổn thương. Phải chắc chắn rằng, bạn tuỳ biến tất cả các phương án quét theo mạng hoặc theo cấu hình của hệ thống để tiết kiệm đáng kể khoảng cách dải tần và nguồn lực cũng như để có kết quả quét chính xác hơn. Sau đó nhấp **Bắt đầu quét**.

Khi quá trình quét kết thúc, Nessus sẽ hiển thị các khám phá và đưa ra các khuyến cáo. Bạn có thể lưu lại báo cáo ở nhiều dạng, kể cả HTML với các hình tròn và các biểu đồ. Bạn có thể xem các báo cáo được lưu trong phần trình duyệt mà bạn muốn.

12.7. Kiểm tra độ mạnh của RAM trong Hệ thống của bạn

Khi hệ thống của bạn có một hành vi không được mong đợi (treo hoặc tự khởi động lại hết lần này đến lần khác), như vậy có thể có vấn đề với bộ nhớ. Bạn có thể thử các module RAM modules bằng chương trình **memtest**, như được miêu tả dưới đây.

Khởi động máy tính của bạn và khởi phát chương trình từ đĩa CD LinuxDefender. Đánh vào **kiểm tra bộ nhớ** khi khởi động và nhấn Enter.

Chương trình Kiểm tra Bộ nhớ (Memtest)sẽ khởi động ngay lập tức và sẽ tiến hành một số thử nghiệm để kiểm tra tình trạng RAM. Bạn có thể cấu hình những gì phải kiểm tra để vận hành các phương án khác của Memtest bằng cách nhấn `c`.

Một lần kiểm tra bộ nhớ hoàn chỉnh phải mất tới 8 giờ, tuỳ thuộc vào công suất và tốc độ RMA trong các hệ thống của bạn. Chúng tôi khuyến cáo bạn nên để cho Memtest chạy tất cả các chương trình kiểm tra của mình để xác định được toàn bộ tất cả các lỗi về RAM. Bạn có thể thoát bất cứ lúc nào bằng cách nhấn vào `ESC`

Nếu bạn có ý đọnh mua một phần cứng mới (Một hệ thống hoàn chỉnh hoặc chỉ một số hợp phần) bạn nên sử dụng LinuxDefender và memtest để kiểm tra lỗi hoặc tính tương thích của chúng.

Nhận trợ giúp

13. Hỗ trợ

13.1. Bộ phận 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.

13.2. Trợ giúp trên mạng

13.2.1. 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.

13.3. Thông tin để liên lạc

Thông tin hiệu quả là chìa khoá cho sự thành công trong kinh doanh. Trong 10 năm qua, SOFTWIN 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.

13.3.1. Các địa chỉ Web

Sales department: <sales@bitdefender.com>
<support@bitdefender.com>
Documentation: <documentation@bitdefender.com>
<support@bitdefender.com>
Marketing: <marketing@bitdefender.com>
Media Relations: <pr@bitdefender.com>
<support@bitdefender.com>
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

13.3.2. 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.

Đức

Softwin GmbH
Đại bản doanh Tây Âu
Karlsdorferstrasse 56
88069 Tettnang
Đức
Tel: +49 7542 9444 44
Fax: +49 7542 9444 99
Email: <info@bitdefender.com>
Sales: <sales@bitdefender.com>
Web: http://www.bitdefender.com
Technical Support: <support@bitdefender.com>

UK and Ireland

One Victoria Square
Birmingham
B1 1BD
Tel: +44 207 153 9959
Fax: +44 845 130 5069
Email: <info@bitdefender.com>
Sales: <sales@bitdefender.com>
Web: http://www.bitdefender.co.uk
<support@bitdefender.com>

Tây ban nha

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Technical support:
Email: <support@bitdefender.com>
Customer Service: 954-776-6262
http://www.bitdefender.com

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

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 tập 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.