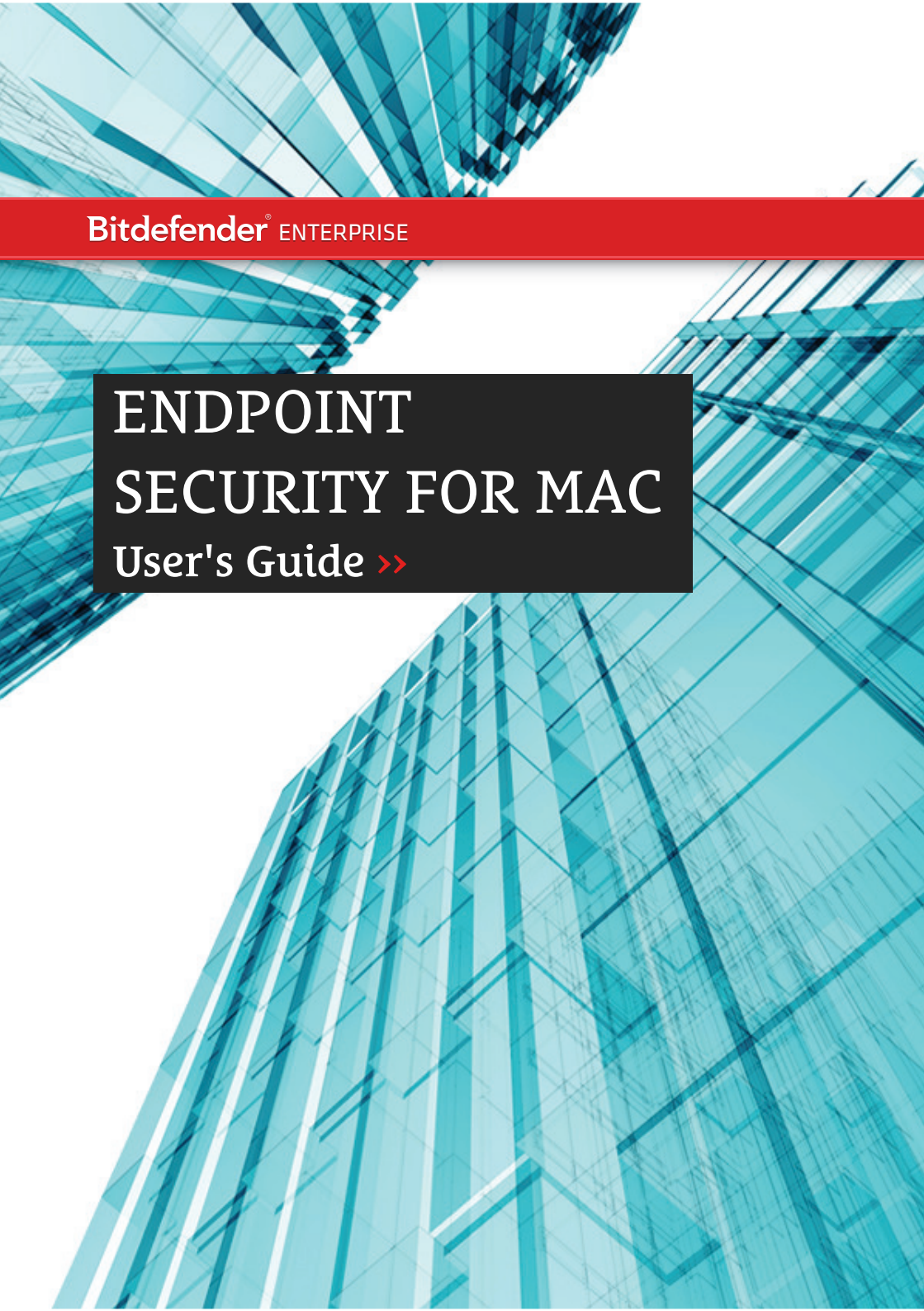

Bitdefender® ENTERPRISE
ENDPOINT SECURITY FOR MAC
User's Guide ››

Endpoint Security for Mac
User's Guide

Publication date 2014.02.04

Copyright© 2014 Bitdefender

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.

Bitdefender

Table of Contents

Using This Guide ..... **v**
1. Purpose and Intended Audience v
2. How to Use This Guide v
3. Conventions Used in This Guide v
3.1. Typographical Conventions v
3.2. Admonitions vi
4. Request for Comments vi

1. Getting Started **1**
1.1. About Endpoint Security for Mac 1
1.2. Opening Endpoint Security for Mac 1
1.3. Application Main Window 2
1.4. Application Dock Icon 3

2. Protecting against Malicious Software **4**
2.1. Best Practices 4
2.2. Scanning Your Mac 4
2.3. Scan Wizard 5
2.4. Fixing Issues 6
2.5. Quarantine 7
2.6. Web protection 8
2.7. Updates 9
2.7.1. Requesting an Update 9
2.7.2. Getting Updates through a Proxy Server 9
2.7.3. Update to a new version 10

3. Configuring Preferences **11**
3.1. Accessing Preferences 11
3.2. General Preferences 11

4. Frequently Asked Questions **12**

5. Getting Help **14**

Types of Malicious Software **15**

Using This Guide

1. Purpose and Intended Audience

This documentation is intended for the end users of **Endpoint Security for Mac**, the Security for Endpoints client software installed on computers to protect them against malware and other Internet threats. The information presented herein should be easy to understand by anyone who is able to work under Macintosh.

You will find out how to configure and use Endpoint Security for Mac to protect your computer against viruses and other malicious software. You will learn how to get best from Bitdefender.

We wish you a pleasant and useful lecture.

2. How to Use This Guide

This guide is organized around several major topics:

Getting Started (p. 1)
Get started with Endpoint Security for Mac and its user interface.

Protecting against Malicious Software (p. 4)
Learn how to use Endpoint Security for Mac to protect your computer against malicious software.

Configuring Preferences (p. 11)
Learn more about the Endpoint Security for Mac preferences.

Getting Help (p. 14)
Where to look and where to ask for help if something unexpected appears.

3. Conventions Used in This Guide

3.1. Typographical Conventions

Several text styles are used in this guide for an improved readability. Their aspect and meaning are presented in the table below.

Appearance	Description
`sample syntax`	Syntax samples are printed with `monospaced` characters.

Appearance	Description
http://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
documentation@bitdefender.com	E-mail addresses are inserted in the text for contact information.
Using This Guide (p. v)	This is an internal link, towards some location inside the document.
`filename`	File and directories are printed using `monospaced` font.
option	All the product options are printed using **bold** characters.
keyword	Important keywords or phrases are highlighted using **bold** characters.

3.2. Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.

Note
The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.

Important
This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.

Warning
This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

4. Request for Comments

We invite you to help us improve the book. We have tested and verified all of the information to the best of our ability. Please write to tell us about any flaws you find in this book or how you think it could be improved, to help us provide you with the best documentation possible.

Let us know by sending an e-mail to documentation@bitdefender.com. Please write all of your documentation-related e-mails in English so that we can process them efficiently.

1. Getting Started

This chapter includes the following topics:

- About Endpoint Security for Mac (p. 1)
- Opening Endpoint Security for Mac (p. 1)
- Application Main Window (p. 2)
- Application Dock Icon (p. 3)

1.1. About Endpoint Security for Mac

Endpoint Security for Mac is a fully-automated computer security program, managed remotely by your network administrator. Once installed, it protects you against all kinds of malware, inlcuding viruses, spyware, trojans, keyloggers, worms and adware. It can also be used to enforce your organization's computer and Internet use policies.

This app detects and removes not only Mac malware, but also Windows malware, thus preventing you from accidentally sending infected files to your family, friends and colleagues using PCs.

1.2. Opening Endpoint Security for Mac

You have several ways to open Endpoint Security for Mac.

- Click the Endpoint Security for Mac icon in the Launchpad.
- Open a Finder window, go to `Applications` and double-click the `Endpoint Security for Mac` icon.

  Alternatively, you can use Spotlight to find and open the application.

1.3. Application Main Window

In the application's main window you can take important actions to improve your system protection. You can check your computer's security status and secure your web browsing experience.

Application Main Window

The status bar at the top of the window informs you about the system's security status using explicit messages and suggestive colors. If Endpoint Security for Mac has no warnings, the status bar has shades of green. When a security issue has been detected, the status bar green shades are replaced with yellow shades. It may also include an action button to help you quickly fix the issue. For detailed information on issues and how to fix them, refer to Fixing Issues (p. 6).

Under the status bar, four scan buttons are available to help you scan your Mac:

- **Scan Critical Locations** - checks for malware the most vulnerable locations on your system (for example, the folders that contain the documents, downloads, mail downloads and temporary files of each user).
- **Full System Scan** - performs a comprehensive check for malware of the entire system. All connected mounts will be scanned too.
- **Scan a Custom Location** - helps you check specific files, folders or volumes for malware.
- **Continuous Scan** - continuously monitors the applications running on the computer, looking for malware-like actions and prevents new malware threats from entering your system. Continuous Scan is controlled by your network administrator via security policies.

For more information, refer to Scanning Your Mac (p. 4).

Besides the scan buttons, additional options are available:

- **Web protection** - filters all web traffic and blocks any malicious content to secure your web browsing experience. For more information, refer to Web protection (p. 8).

1.4. Application Dock Icon

The Endpoint Security for Mac icon can be noticed in the Dock as soon as you open the application. The icon in the Dock provides you with an easy way to scan files and folders for malware. Just drag and drop the file or folder over the Dock icon and the scan will start immediately.

Dock Icon

2. Protecting against Malicious Software

This chapter includes the following topics:

- Best Practices (p. 4)
- Scanning Your Mac (p. 4)
- Scan Wizard (p. 5)
- Fixing Issues (p. 6)
- Quarantine (p. 7)
- Web protection (p. 8)
- Updates (p. 9)

2.1. Best Practices

To keep your system malware-free and to prevent accidental infection of other systems, follow these best practices:

- Check and fix the issues reported by Endpoint Security for Mac regularly. For detailed information, refer to Fixing Issues (p. 6).
- You should also adhere to these best practices:
  - Make a habit of scanning files that you download from an external storage memory (such as an USB stick or a CD), especially when you do not know the source.
  - If you have a DMG file, mount it and then scan its contents (the files within the mounted volume/image).

  The easiest way to scan a file, a folder or a volume is to drag&drop it over the Endpoint Security for Mac window or Dock icon.

No other configuration or action is required.

2.2. Scanning Your Mac

You can scan your Mac or specific files anytime you want.

The easiest way to scan a file, a folder or a volume is to drag&drop it over the Endpoint Security for Mac window or Dock icon. The scan wizard will appear and guide you through the scanning process.

You can also start a scan as follows:

1. Open Endpoint Security for Mac.
2. Click one of the three scan buttons to start the desired scan.
   - **Scan Critical Locations** - checks for malware the most vulnerable locations on your system (for example, the folders that contain the documents, downloads, mail downloads and temporary files of each user).
   - **Full System Scan** - performs a comprehensive check for malware of the entire system. All connected mounts will be scanned too.

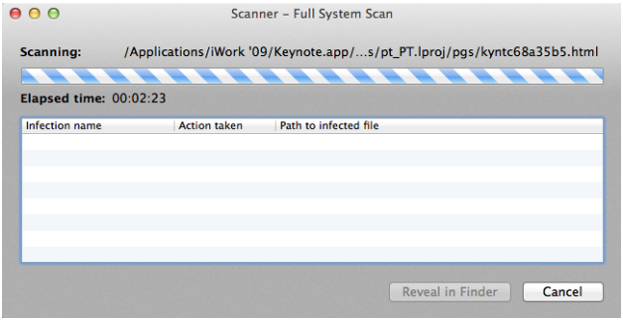
     Note

     Depending on the size of your hard disk, scanning the entire system may take a while (up to an hour or even more). For improved performance, it is recommended not to run this task while performing other resource-intensive tasks (such as video editing).

   - **Scan a Custom Location** - helps you check specific files, folders or volumes for malware.
   - **Continuous Scan** - continuously monitors the applications running on the computer, looking for malware-like actions and prevents new malware threats from entering your system. Continuous Scan is controlled by your network administrator via security policies.

2.3. Scan Wizard

Whenever you initiate a scan, the Endpoint Security for Mac scan wizard will appear.



Scanning in Progress

You can see real-time information about the scan. Detected threats and the action taken on them are displayed in the Scan results section.

Wait for Endpoint Security for Mac to finish scanning.

Note
The scanning process may take a while, depending on the complexity of the scan.

2.4. Fixing Issues

Endpoint Security for Mac automatically detects and informs you about a series of issues that can affect the security of your system and data. In this way, you can fix security risks easily and in a timely manner.

Fixing the issues indicated by Endpoint Security for Mac is a quick and easy way to ensure minimum protection of your system and data.

Detected issues include:

- The new malware signatures and product updates have not been downloaded from Bitdefender servers.
- Unresolved threats have been detected on your system.
- **Continuous Scan** is off. It can be turned-on via security policy only by your network administrator.

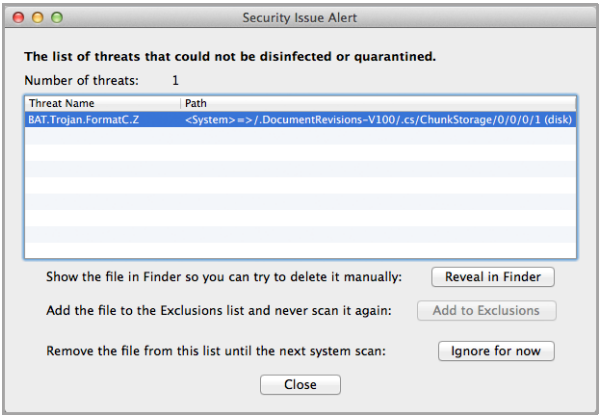
To check and fix detected issues:

1. Open Endpoint Security for Mac.
2. If Endpoint Security for Mac has no warnings, the status bar has shades of green. When a security issue has been detected, the status bar green shades are replaced with yellow shades.
3. Check the description for more information.
4. Depending on the detected issue, a button may be available on the status bar to help you quickly fix it. Click the button to remove the security risk.

Usually, this happens when there are unresolved threats. You can view them and decide what to do with them.

Note

Endpoint Security for Mac can take actions on current user's files only. Infected files owned by other users cannot be cleaned or quarantined by this app. Such files will be reported as unresolved issues.



Unresolved Threats Window

The list of unresolved threats is updated after each system scan.

You can choose to take the following actions on unresolved threats:

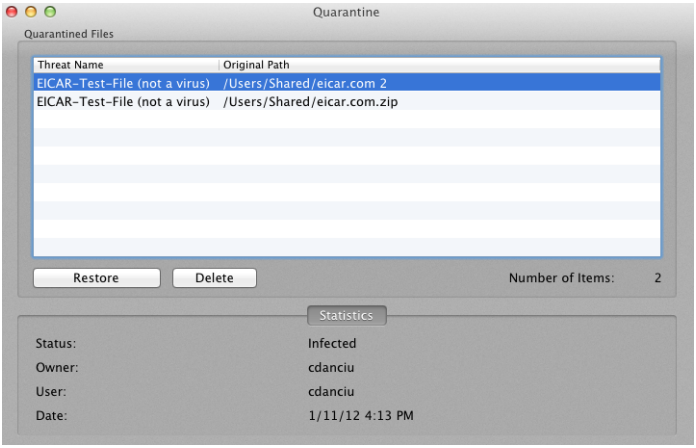
- Reveal in Finder. Take this action to remove the infections manually.
- Ignore for now. The issue will be removed from the status bar until the next scan.

2.5. Quarantine

Endpoint Security for Mac allows isolating the infected or suspicious files in a secure area, named quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

To view and manage the quarantined files, open the Quarantine window:

1. Open Endpoint Security for Mac.
2. Click **Actions** in the menu bar.
3. Choose **View Quarantine**.



Quarantined Files

The Quarantine section displays all the files currently isolated in the Quarantine folder.

To delete a file from quarantine, select it and click **Delete**. If you want to restore a quarantined file to its original location, select it and click **Restore**.

2.6. Web protection

Endpoint Security for Mac uses the TrafficLight extensions to completely secure your web browsing experience. The TrafficLight extensions intercept, process and filter all web traffic, blocking any malicious content.

The extensions work and integrate with the following web browsers: Mozilla Firefox, Google Chrome and Safari.

An array of features is available to protect you from all kinds of threats you may encounter while web browsing:

- Advanced Phishing Filter - prevents you from accessing websites used for phishing attacks.
- Malware Filter - blocks any malware you come in contact with while browsing the Internet.
- Search Results Analyzer - provides advance warning of risky websites within your search results.
- Antifraud Filter - provides protection against fraudulent websites while browsing the Internet.
- Tracker Notification - detects trackers on the visited web pages protecting your online privacy.

To enable the TrafficLight extensions, follow these steps:

1. Open Endpoint Security for Mac.
2. Click **Activate** to activate the Web protection.
3. Endpoint Security for Mac will detect what web browser you have installed on your system. To install the TrafficLight extension on your browser, click **Get extension**.
4. You will be redirected to this online location:
   http://bitdefender.com/solutions/trafficlight.html
5. Select **Free Download**.
6. Follow the steps to install the TrafficLight extension corresponding to your web browser.

2.7. Updates

New malware is found and identified every day. This is why it is very important to keep Endpoint Security for Mac up to date with the latest malware signatures.

While the **Continuous Scan** is controlled via security policy, the malware signatures and product updates are automatically downloaded on your system. If your network administrator disables the Continuous Scan control via policy, you will have to keep the **Continuous Scan** button enabled to allow the malware signatures and product updates to be automatically downloaded on your system.

The malware signatures update is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update will not affect the product operation and, at the same time, any vulnerability will be excluded.

2.7.1. Requesting an Update

You can request an update manually anytime you want. Update by user request is recommended before you start a comprehensive scan.

An active Internet connection is required in order to check for available updates and download them.

To request an update manually:

1. Open Endpoint Security for Mac.
2. Click the **Actions** in the menu bar.
3. Choose **Update Virus Database**.

You can see the update progress and downloaded files.

2.7.2. Getting Updates through a Proxy Server

Endpoint Security for Mac can update only through proxy servers that do not require authentication. You do not have to configure any program settings.

If you connect to the Internet through a proxy server that requires authentication, you must switch to a direct Internet connection regularly in order to obtain malware signature updates.

2.7.3. Update to a new version

Occasionally, we launch product updates to improve the product functionalities. These updates may require a system restart in order to initiate the installation of new files. By default, if an update requires a computer restart, Endpoint Security for Mac will keep working with the previous files until you reboot the system. In this case, the update process will not interfere with the user's work.

When a product update is completed, a pop-up window will inform you to restart the system. If you miss this notification, you can either click **Restart to upgrade** from the menu bar or manually restart the system.

3. Configuring Preferences

This chapter includes the following topics:

- Accessing Preferences (p. 11)
- General Preferences (p. 11)

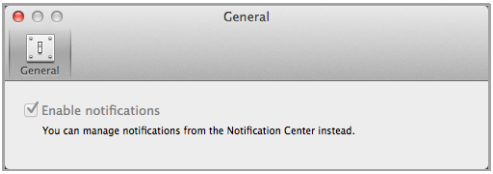
3.1. Accessing Preferences

To open the Endpoint Security for Mac Preferences window:

1. Open Endpoint Security for Mac.
2. Do any of the following:
   - Click Endpoint Security for Mac in the menu bar and choose **Preferences**.
   - Press Command-Comma(,).

3.2. General Preferences

The general preferences allow you to configure the general behavior of the application.



General Preferences

- **Enable notifications.** Allows you to receive notifications regarding Endpoint Security for Mac events and activities. On systems 10.8 and up, you will automatically be notified through Notification Center. On systems 10.7, you will be notified in Growl, if the application is installed. If you do not have Growl installed, you will still receive notifications through Endpoint Security for Mac notification mechanism. Integration with Growl is an extra feature and it does not affect in any way your Endpoint Security for Mac product.

Note

Growl is a third-party application developed by The Growl Project. It is not installed by default on Mac OS X. You can find out more information and download Growl from http://growl.info/.

4. Frequently Asked Questions

The scan log indicates there are still unresolved items. How do I remove them?

The unresolved items in the scan log may be:

- restricted access archives (xar, rar, etc.)

  Solution: Use the **Reveal in Finder** option to find the file and delete it manually. Make sure to empty the Trash.

- restricted access mailboxes (Thunderbird, etc.)

  Solution: Use the application to remove the entry containing the infected file.

- files owned by another user

  Solution: Use the **Reveal in Finder** option to find the file and contact the owner to find out if it is safe to remove that file. If it is safe to remove the file, delete it manually. Make sure to empty the Trash.

Note

Restricted access files means files Endpoint Security for Mac can only open, but it cannot modify them.

Can I update Endpoint Security for Mac through a Proxy Server?

Endpoint Security for Mac can update only through proxy servers that do not require authentication. You do not have to configure any program settings.

If you connect to the Internet through a proxy server that requires authentication, you must switch to a direct Internet connection regularly in order to obtain malware signature updates.

How do I remove the TrafficLight extensions from my web browser?

- To remove the TrafficLight extensions from Mozilla Firefox, follow these steps:
  1. Open your Mozilla Firefox browser.
  2. Go to **Tools** and select **Add-ons**.
  3. Select **Extensions** on the left column.
  4. Select the extension and click **Remove**.
  5. Restart the browser for the removal process to complete.
- To remove the TrafficLight extensions from Google Chrome, follow these steps:
  1. Open your Google Chrome browser.

2. Click on the browser toolbar.
3. Go to **Tools** and select **Extensions**.
4. Select the extension and click **Remove**.
5. Click **Uninstall** to confirm the removal process.

- To remove Bitdefender TrafficLight from Safari, follow these steps:
  1. Open your Safari browser.
  2. Click on the browser toolbar and click **Preferences**.
  3. Select the **Extensions** tab and find the **Bitdefender TrafficLight on Safari** extension in the list.
  4. Select the extension and click **Uninstall**.
  5. Click **Uninstall** to confirm the removal process.

5. Getting Help

For any problems or questions concerning Endpoint Security for Mac, please contact your network administrator.

Open **About Endpoint Security for Mac** window to find product and contact information:

- Open Endpoint Security for Mac.
- Click **Endpoint Security for Mac** in the menu bar.
- Choose **About Endpoint Security for Mac**.

Types of Malicious Software

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Keylogger

A keylogger is an application that logs anything you type.

Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.