

F-Secure Anti-Virus **2013**

目录

第 1 章： 安装.....	5
首次安装前的说明.....	6
首次安装本产品.....	6
安装和升级应用程序.....	6
帮助与支持.....	7
 第 2 章： 使用入门.....	 9
如何使用自动更新.....	10
检查更新状态.....	10
更改我的互联网连接设置.....	10
检查实时保护网络的状态.....	11
如何查看产品进行了哪些操作.....	11
查看通知历史记录.....	11
更改通知设置.....	11
实时保护网络.....	12
什么是“实时保护网络”.....	12
“实时保护网络”优点.....	12
您将提供哪些数据.....	13
我们如何保护您的隐私.....	14
成为“实时保护网络”的参与者.....	14
有关“实时保护网络”的问题.....	14
如何知道我的订购是否有效.....	15
操作中心.....	15
激活订购.....	15
 第 3 章： 介绍.....	 17
查看个人保护的总体状态.....	18
查看产品统计信息.....	18
处理产品更新.....	19
查看数据库版本.....	19
更改移动宽带设置.....	19
什么是病毒和其他恶意软件.....	20
病毒.....	20
间谍软件.....	20
Rootkit.....	21

危险软件.....	21
第 4 章： 保护我的计算机免受恶意软件威胁.....	23
如何扫描我的计算机.....	24
自动扫描文件.....	24
手动扫描文件.....	26
扫描电子邮件.....	29
查看扫描结果.....	29
如何将文件排除在扫描范围之外.....	30
排除文件类型.....	30
按位置排除文件.....	30
查看排除的应用程序.....	31
如何使用隔离区.....	32
查看隔离的项目.....	32
还原已隔离项目.....	32
什么是 DeepGuard.....	33
开启或关闭 DeepGuard.....	33
允许 DeepGuard 已阻止的应用程序.....	33
在兼容模式下使用 DeepGuard.....	34
如何处理可疑行为警告.....	34

安装

主题:

[首次安装前的说明](#)
[首次安装本产品](#)
[安装和升级应用程序](#)
[帮助与支持](#)

首次安装前的说明

感谢您选用 F-Secure。


若要安装产品，您需要下列项目：

安装光盘或安装程序包。若您使用的是不带光驱的上网本，您可从网站 www.f-secure.com/netbook 下载安装程序包。

您的订购密钥。

互联网连接。

若您已有其他供应商的安全产品，安装程序将会试图自动将其删除。若未自动删除，请手动将其删除。

 **注意：**若您在计算机上拥有多个帐户，请在安装时使用有管理员权限的帐户登录。

首次安装本产品

产品安装说明。

请按以下说明安装产品：

1. 插入光盘或双击下载的安装程序。

若光盘未自动启动，请转至 Windows 资源管理器，先后双击 CD-ROM 图标和安装文件以开始安装。

2. 请按照屏幕上的说明操作。

如果从商店购买产品光盘，您可在《快速安装指南》封面上找到订购密钥。


如果从 F-Secure 网上商店下载本产品，则可在购买订单的确认电子邮件中找到订购密钥。

您可能需要重启计算机，然后才可验证订购并从互联网下载最新更新。若从光盘安装，请记得在重启计算机前取出安装光盘。

安装和升级应用程序

新订购激活说明。

按照以下说明激活您的新订购，或使用启动栏安装新应用程序：

 **注意：**您可在 Windows 系统托盘上找到启动栏图标。

1. 在启动栏上，右键单击最右侧的图标。
弹出窗口菜单将打开。
2. 选择 [查看我的订购](#)。
3. 在 [我的订购](#) 下，转至 [订购状态](#) 页面，然后单击 [激活订购](#)。
[激活订购](#) 窗口将打开。
4. 输入您的应用程序订购密钥，然后单击 [确定](#)。
5. 验证并激活订购后，单击 [关闭](#)。
6. 在 [我的订购](#) 下，转至 [安装状态](#) 页面。若安装未自动开始，请按以下说明操作：

- a) 单击 [安装](#)。
安装窗口将打开。
- b) 单击 [下一步](#)。
应用程序已下载，安装开始。
- c) 安装完成后，单击 [关闭](#)。

新订购已激活。

帮助与支持

单击“帮助”图标或在产品的任何画面下按 F1，即可访问产品联机帮助。

注册后，您便有权使用免费产品更新、产品支持等其他服务。您可在 www.f-secure.com/register 注册。

使用入门

主题：

[如何使用自动更新](#)

[如何查看产品进行了哪些操作](#)

[实时保护网络](#)

[如何知道我的订购是否有效](#)

有关本产品快速入门方法的信息。

本节介绍如何通过启动栏来更改公用设置和管理您的订购。

启动栏的公用设置是指应用于安装在启动栏上所有程序的设置。无需分别更改每个程序的设置，您只要编辑公用设置，所有已安装程序都会使用该设置。

启动栏的公用设置包括：

下载，可在此查看已下载更新的信息，并手动检查是否有新的更新可用。

连接设置，可在此更改计算机连接互联网的方式。

通知，可在此查看过去的通知并设置您想要查看的通知类型。

隐私设置，可在此选择是否允许计算机连接至实时保护网络。

您也可通过启动栏来管理已安装程序的订购。

如何使用自动更新

自动更新可以使计算机上的防护保持最新。

本产品会在计算机连接到互联网时检索最新更新。它可检测网络流量，即使网络连接速度很慢时也不会干扰其他互联网的使用。

检查更新状态

查看最新更新的日期和时间。

如果开启了自动更新，则计算机连接到互联网时，产品会自动接收最新的更新。

确保已进行最新更新：

1. 在启动栏上，右键单击最右侧的图标。
将显示弹出菜单。
2. 选择[打开公用设置](#)。
3. 选择[自动更新](#) > [下载](#)。
4. 单击[立即检查](#)。

产品会连接到互联网并检查最新的更新。如果计算机未受到最新保护，产品会检索最新更新。

 **注意：**如果正使用调制解调器或已开启与互联网的 ISDN 连接，则检查更新前须启动连接。


更改我的互联网连接设置

通常无需更改默认设置，但您可以配置服务器连接至互联网的方式，以自动接收更新。

更改互联网连接设置的步骤：


1. 在启动栏上，右键单击最右侧的图标。
将显示弹出菜单。
2. 选择[打开公用设置](#)。
3. 选择[自动更新](#) > [连接](#)。
4. 在[互联网连接](#)列表中，选择计算机连接至互联网的方式。

如果计算机一直连接网络，请选择[假定始终连接](#)。

 **注意：**如果计算机实际上没有一直连接网络而是设置为指定拨号，则选择[假定始终连接](#)会导致多次拨号。

仅在产品检测到活动的网络连接时，方可选择[检测连接](#)以检索更新。

仅在产品检测到其他网络流量时，选择[检测流量](#)，以检索更新。

 **提示：**如果采用非通用硬件配置如[检测连接](#)设置之后，即使在无网络连接时仍检测到网络连接在使用中，则请选择[检测流量](#)。

5. 在[HTTP 代理服务器](#)列表中，选择计算机是否使用[代理服务器](#)连接至互联网。

如果计算机直接连接互联网，请选择[无 HTTP 代理服务器](#)。

选择[手动配置 HTTP 代理服务器](#)以配置 [HTTP 代理服务器](#)设置。

选择[使用我的浏览器的 HTTP 代理服务器](#)，以使用在 Web 浏览器上已配置的相同的[HTTP 代理服务器](#)设置。

检查实时保护网络的状态

若要正常运行，多种产品功能均取决于实时保护网络的连接状态。

如果发生网络问题，或您的防火墙阻止实时保护网络流量，则状态为“已断开连接”。如果未安装要求访问实时保护网络的产品功能，则状态为“未使用”。

若要查看状态：

1. 在启动栏上，右键单击最右侧的图标。
将显示弹出菜单。
2. 选择[打开公用设置](#)。
3. 选择[自动更新](#) > [连接](#)。

在[实时保护网络](#)下，您可查看实时保护网络的当前状态。

如何查看产品进行了哪些操作

您可在[通知](#)页面上查看本产品为保护计算机所采取的操作。

本产品会在进行操作时（例如发现阻止的病毒时）显示通知。您的服务提供商也会发送一些通知，例如让您了解可用新服务的通知。

查看通知历史记录

您可在通知历史记录中查看显示过的通知。

若要查看通知历史记录：

1. 在启动栏上，右键单击最右侧的图标。
将显示弹出菜单。
2. 选择[打开公用设置](#)。
3. 选择[其他](#) > [通知](#)。
4. 单击[显示通知历史记录](#)。
通知历史记录列表开启。

更改通知设置

您可选择想要产品显示的通知类型。

若要更改通知设置：

1. 在启动栏上，右键单击最右侧的图标。
将显示弹出菜单。
2. 选择[打开公用设置](#)。
3. 选择[其他](#) > [通知](#)。
4. 选择或清除[允许程序消息](#)，以开启或关闭程序消息。

开启此设置后，本产品会显示来自已安装程序的通知。

5. 选择或清除[允许促销消息](#)，以开启或关闭促销消息。
6. 单击[确定](#)。

实时保护网络

本文档介绍 F-Secure Corporation 的一项在线服务“实时保护网络”，该服务可识别安全的应用程序和网站，同时为您提供防护，抵御恶意软件和网站入侵程序的侵害。

什么是“实时保护网络”

“实时保护网络”是一种针对基于互联网的最新威胁提供快速响应的在线服务。

作为“实时保护网络”的参与者，您可以帮助我们提高抵御新威胁的能力。“实时保护网络”收集某些未知、恶意或可疑应用程序的统计信息，以及它们在您设备上所执行的操作。此信息会匿名发送至 F-Secure Corporation，以供联合数据分析。我们使用经分析的信息来提高您设备的安全性，以抵御最新威胁和恶意文件的侵害。

“实时保护网络”如何运作

作为“实时保护网络”的参与者，您可以提供关于未知应用程序和网站、网站上恶意应用程序和入侵程序的信息。“实时保护网络”不会追踪您的网页活动或收集已分析网站的信息，也不会收集安装于您计算机上的安全应用程序的相关信息。

如果您不想提供此类数据，则“实时保护网络”不会收集已安装应用程序或已访问网站的信息。但是，产品需要向 F-Secure 服务器查询应用程序、网站、邮件和其他对象的声誉。该查询使用加密校验和执行，被查询的对象本身不会发送至 F-Secure。我们不会按用户追踪数据；仅文件或网站计数器的计数会增加。

不可能完全停止至“实时保护网络”的所有网络流量，因为它是产品所提供保护的必要部分。

“实时保护网络”优点

使用“实时网络保护”，可更快更准确地抵御最新威胁，且您不会收到针对非恶意的可疑应用程序不必要的警报。

作为“实时保护网络”的参与者，您可以帮助我们发现新恶意软件和未检测到的恶意软件，以及消除病毒定义数据库可能出现的误报情况。

“实时保护网络”的所有参与者互相帮助。“实时保护网络”在设备上发现可疑应用程序时，如果在其他设备上已发现同样的应用程序，您将可利用其分析结果。“实时保护网络”可提高设备的整体性能，因为安装的安全产品不需要扫描“实时保护网络”已分析并认定为安全的应用程序。同样的，恶意网站以及大量未经请求邮件的相关信息可通过“实时保护网络”共享，让我们能够为您提供更准确的防护，抵御网站入侵程序和垃圾邮件的侵害。

参与“实时保护网络”的人越多，个人参与者受到的保护就越全面。

您将提供哪些数据

作为“实时保护网络”的参与者，您可提供设备上所存储应用程序以及您所访问网站的相关信息，以便“实时保护网络”为您提供防护，抵御最新恶意应用程序和可疑网站的侵害。

分析文件声誉

“实时保护网络”仅收集声誉未知的应用程序的相关信息，以及怀疑或已知为恶意软件的文件的相关信息。

“实时保护网络”会收集设备上的安全和可疑应用程序的匿名信息。“实时保护网络”仅收集可执行文件的信息（例如，在 Windows 平台上，扩展名为 .cpl、.exe、.dll、.ocx、.sys、.scr、.drv 的可移植可执行文件）。

收集的信息包括：

- 设备中应用程序的文件路径、
- 文件大小及其创建或修改时间、
- 文件属性和权限、
- 文件签名信息、
- 文件的当前版本以及创建该文件的公司、
- 文件来源或其下载 URL、
- 已扫描文件的 F-Secure DeepGuard 和防病毒分析结果，以及
- 其他类似信息。

“实时保护网络”绝不会收集个人文档的任何信息，除非发现这些文档受到感染。对于任何类型的恶意文件，“实时保护网络”会收集感染的名称以及文件的杀毒状态信息。

通过“实时保护网络”，您还可提交可疑应用程序以供分析。您提交的应用程序应仅包含可移植可执行文件。“实时保护网络”绝不会收集任何个人文档信息，也决不会自动上载此类信息以供分析。

提交文件以供分析

使用“实时保护网络”，您还可提交可疑的应用程序以供分析。


您可以在产品提示时，手动提交单个可疑应用程序。您还可以提交可移植可执行文件。“实时保护网络”将不会上传您的个人文档。

分析网站声誉

“实时保护网络”不会跟踪您的网络活动，不会收集已分析网站的相关信息。它会在您浏览网络时确保访问的网站为安全网站。浏览网站时，“实时保护网络”会检查其安全性，并在网站被评定为可疑或有害网站时通知您。

如果您访问的网站包含恶意或可疑内容，或包含已知入侵程序，则“实时保护网络”会收集网站的完整 URL，以便对网页内容予以分析。

如果您访问未经评定的网站，则“实时保护网络”会收集域和子域的名称，在某些情况下还会收集所访问网页的路径，以便能分析和评定网站。为保护您的隐私，若任何 URL 参数中可能包含可通过个人身份识别方式识别出您身份的信息，则我们会将此参数删除。

 **注意：**“实时保护网络”不会评定或分析专用网络中的网页，因此绝不会收集专用 IP 网络地址（例如企业内部网）上的任何信息。

分析系统信息

“实时保护网络”收集操作系统的名称和版本、互联网连接信息以及“实时保护网络”使用情况统计信息（例如，查询网站声誉的次数以及查询返回结果的平均时间），以便我们可监控和改善服务。

我们如何保护您的隐私

我们安全地传输信息，并自动删除数据中可能包含的任何个人信息。

“实时保护网络”删除身份识别数据后，再将数据发送至 F-Secure，并在传输过程中加密所有收集的信息，以防止其遭到未经授权的访问。收集的信息不会单独予以处理，而是与其他“实时网络保护”参与者所提供的信息一起集中处理。所有数据将受到匿名统计分析，这意味着不会有任何数据以任何方式泄露您的隐私。

收集的数据中不会包含可供识别您个人身份的任何信息。“实时保护网络”不会收集 IP 地址或其他私人信息，如电子邮件地址、用户名和密码。虽然我们竭力删除所有可识别个人身份的数据，但可能仍有某些身份识别数据遗留在收集的信息中。在这种情况下，我们不会设法使用这些无意中收集的数据来识别您的身份。

在已收集信息的传输、存储和处理过程中，我们将采用严格的安全措施，以及实体、管理和技术保障措施来保护收集的信息。信息将存储于安全位置，以及我们或我们转包商办公室内由我们控制的服务器上。仅授权人员可访问收集的信息。

F-Secure 可能与其子公司、转包商、分销商和合作伙伴共享收集的数据，但始终会采用无法识别个人身份的匿名形式共享。

成为“实时保护网络”的参与者

您可以通过提供恶意程序和网站的信息，来帮助我们改善“实时保护网络”的防护功能。

在安装过程中，您可以选择参与“实时保护网络”。使用默认安装设置，您可以向“实时保护网络”提供数据。您可以稍后在产品中更改此设置。

请按以下说明更改“实时保护网络”设置：

1. 在启动栏上，右键单击最右侧的图标。
将显示弹出菜单。
2. 选择 [打开公用设置](#)。
3. 选择 [其他](#) > [隐私](#)。
4. 勾选“参与”复选框以成为“实时保护网络”参与者。

有关“实时保护网络”的问题

了解“实时保护网络”任何相关问题的联系信息。

如果您对“实时保护网络”有任何其他问题，请联系：

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 赫尔辛基

芬兰

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

我们网站上将始终提供此策略的最新版本。

如何知道我的订购是否有效

您的订购类型和状态显示在[订购状态](#)页面上。

如果订购即将过期或者已过期，相应启动栏图标上的程序整体保护状态将会随之发生改变。

检查订购有效性：

1. 在启动栏上，右键单击最右侧的图标。
将显示弹出菜单。
2. 选择[查看我的订购](#)。
3. 选择[订购状态](#)，以查看已安装程序的订购信息。
4. 选择[安装状态](#)以查看有哪些可用的程序可安装。

您的订购状态和到期日期也会显示在程序的[统计信息](#)页面上。如果您的订购已过期，您需要续订以便继续接受更新和使用本产品。

 **注意：**在您的订购过期后，产品状态图标会在系统任务栏上闪烁。

操作中心

操作中心显示您需注意的任何重要通知。

如果您的订购已过期或即将过期，则操作中心会通知您。操作中心消息的背景色和内容取决于您的订购类型和状态：

如果您的订购即将过期，且有可用的免费订购，则消息会使用白色背景，且包含[激活](#)按钮。

如果您的订购即将过期，且没有可用的免费订购，则消息会使用黄色背景，且包含[购买](#)和[输入密钥](#)按钮。

如果您已购买新的订购，则可单击[输入密钥](#)以提供订购密钥，并激活新订购。

如果您的订购已过期，且有可用的免费订购，则消息会使用红色背景，且包含[激活](#)按钮。

如果您的订购已过期，且没有可用的免费订购，则消息会使用红色背景，且包含[购买](#)和[输入密钥](#)按钮。如果您已购买新的订购，则可单击[输入密钥](#)以提供订购密钥，并激活新订购。


 **注意：**操作中心的[显示通知历史记录](#)链接中会显示产品通知消息列表，而非之前的操作中心消息。

激活订购

若有新的产品订购密钥或活动代码，您需要将其激活。

若要激活订购：

1. 在启动栏上，右键单击最右侧的图标。
将显示弹出菜单。
2. 选择[查看我的订购](#)。
3. 选择下列其中一个操作：
 - 单击[激活订购](#)。
 - 单击[激活市场活动代码](#)。
4. 在打开的对话框中输入新的订购密钥或活动代码，并单击[确定](#)。

 提示：如果已通过电子邮件收到订购密钥，则可从电子邮件中复制密钥，并粘贴到字段中。

输入新的订购密钥后，新订购的有效日期会显示在[订购状态](#)页面上。

介绍

主题：

[查看个人保护的总体状态](#)

[查看产品统计信息](#)

[处理产品更新](#)

[什么是病毒和其他恶意软件](#)

本产品可保护您的计算机免遭病毒和其他有害应用程序的威胁。

产品自动扫描文件、分析应用程序并进行更新。您无需执行任何操作。

查看个人保护的总体状态

[状态](#)页面将显示已安装产品功能的快速概览以其当前状态。

若要打开[状态](#)页面：

在主页面上，单击[状态](#)。

[状态](#)页面将打开。

图标为您显示程序及其安全功能的状态。

状态图标	状态名称	描述
	确定	您的计算机已经受到保护。该功能已开启，并且运作正常。
	信息	产品将通知您功能的特殊状态。 例如，功能正在更新。
	警告	计算机未受到全面保护。 例如，产品长时间未收到更新，或需要留意功能的状态。
	错误	计算机未受保护。 例如，您的订购已过期或关键功能已关闭。
	关闭	非关键功能已关闭。

查看产品统计信息

您可以在[统计信息](#)页面中查看自产品安装完成以来进行的操作。

打开[统计信息](#)页面的步骤：

在主页面上，单击[统计信息](#)。

[统计信息](#)页面将打开。

[上次成功更新检查](#)显示最新更新的时间。

[病毒和间谍软件扫描](#)会显示产品自安装后已扫描和清理的文件数目。

[应用程序](#)显示自安装以来 DeepGuard 允许或阻止的程序数量。

[防火墙连接](#)显示自安装以来允许和阻止的连接次数。

[垃圾邮件和网络钓鱼筛选](#)显示产品已检测为有效电子邮件和垃圾邮件的电子邮件数目。

处理产品更新


产品可自动更新防护状态。

查看数据库版本

您可在[数据库更新](#)页面中查看最新更新时间和版本号。

若要打开[数据库更新](#)页面：

1. 在主页上单击[设置](#)。


 **注意：**您需要有管理权限才能更改设置。

2. 选择[其他设置](#) > [数据库版本](#)。


[数据库版本](#)页面显示病毒和间谍软件定义、DeepGuard 以及垃圾邮件和网络钓鱼筛选的最近更新日期及其版本号。

更改移动宽带设置

选择是否要在使用移动宽带时下载安全更新。


 **注意：**此功能仅可在 Microsoft Windows 7 中使用。

默认情况下，在您使用主运营商的网络时，始终会下载安全更新。但是，当您访问其他运营商的网络时，将暂停更新。这是因为，运营商的网络连接价格不同，例如，在不同国家的价格会不同。若要在浏览时节省带宽，且可能的话同时节省成本，您可考虑将此设置保持不变。

 **注意：**此设置仅适用于移动宽带连接。当计算机连接至固定或无线网络时，将自动更新产品。

若要更改设置：

1. 在主页上单击[设置](#)。

 **注意：**您需要有管理权限才能更改设置。

2. 选择[其他设置](#) > [移动宽带](#) > [下载安全更新](#)。

3. 请为移动连接选择首选更新选项：

[仅限我的主运营商网络](#)

在主运营商的网络中会始终下载更新。当您访问其他运营商网络时，将暂停更新。我们建议您选择此选项，以按预期成本保持安全产品的最新状态。

[从不](#)

使用移动宽带时不会下载更新。

[始终](#)


不论使用何种网络，都始终下载更新。若要不考虑成本，来确保计算机始终保持最新安全状态，请选择此选项。

4. 如果您想要在每次离开主运营商网络时分别确认，请选择[每次离开主运营商网络时询问](#)。

已暂停的安全更新

在主运营商的网络之外使用移动宽带时，可能会暂停安全更新。

在此情况下，您可查看屏幕右下角的**已暂停**通知传单。暂停更新的原因是，运营商的网络连接价格不同，例如，在不同的国家价格会不同。若要在浏览时节省宽带，且可能的话同时节省成本，您可考虑将此设置保持不变。但是，如果您仍要更改设置，请单击**更改**链接。

 注意：

此功能仅可在 Microsoft Windows 7 中使用。

什么是病毒和其他恶意软件

恶意软件为专门损坏计算机，或在您不知情的情况下将计算机用于非法目的，或从计算机上窃取信息的程序。

恶意软件会：

- 控制 Web 浏览器，
- 重定向搜索尝试，
- 显示不必要的广告，
- 记录浏览的网站，
- 窃取个人信息如银行信息，
- 使用计算机发送垃圾邮件，及
- 使用您的计算机攻击其他计算机。

此外，它还会降低计算机的运行速度与稳定性。如果计算机运行速度突然变慢，并经常死机，则可能已感染恶意软件。

病毒

病毒指通常可以将自身附在文件上并快速复制自身的程序；它们会更改并取代其他文件的内容，这样可能会损坏您的计算机。

病毒是一种程序，通常会在您不知情的情况下安装。一旦安装，病毒会试图复制自身。病毒会：

- 使用计算机上的某些系统资源，
- 可能会更改或损坏计算机上的文件，
- 可能试图用您的计算机来感染其他计算机，
- 可能允许使用计算机进行非法活动。

间谍软件

间谍软件是指收集您个人信息的程序。

间谍软件会收集以下个人信息：

- 您曾浏览的互联网网站、
- 计算机上的电子邮件地址、
- 密码或
- 信用卡号码。

间谍软件几乎总是未经您明确授权就自行安装。间谍软件通常会与某个有用的程序一同安装，或通过诱导您在令人误解的弹出窗口中单击某个选项而得以安装。

Rootkit

Rootkit 是一种让其他恶意软件变得难以发现的程序。

Rootkit 会隐藏文件与进程。通常，其目的是隐藏计算机上的恶意活动。当 Rootkit 隐藏恶意软件之后，您很难发现计算机上已安装恶意软件。

此产品配备有专门针对 Rootkit 而设计的扫描程序，让恶意软件无法轻易藏身。

危险软件

危险软件并非专为危害您的计算机而设计，但如果使用不当，它也可能危害您的计算机。

危险软件并不是严格意义上的恶意软件。危险软件程序会执行某些有用但是具有潜在危险的功能。

危险软件程序的示例：

- “实时消息”程序（例如 IRC、互联网中继聊天）、
- 通过互联网在计算机间发送文件所用的程序、
- 互联网电话程序，如 VoIP（IP 电话），
- 远程访问软件，例如 VNC、
- 可能试图恐吓或欺骗个人购买仿冒安全软件的恐吓软件，或
- 设计用来绕过光盘检查程序或拷贝保护程序的软件。

如果此程序在您知悉的情况下安装并进行妥善设置，则其损坏计算机的可能性就要小得多。

如果危险软件是在您不知情的情况下安装，则其很可能含有恶意目的，应将其删除。

保护我的计算机免受恶意软件威胁

主题：

[如何扫描我的计算机](#)

[如何将文件排除在扫描范围之外](#)

[如何使用隔离区](#)

[什么是 DeepGuard](#)

病毒和间谍软件扫描会保护您的计算机免受那些可能盗取个人信息、损害计算机或利用计算机实现非法目的的程序的威胁。

默认下，所有类型的恶意软件会在发现后立即处理，以使其无法损害计算机。

默认情况下，病毒和间谍软件扫描会自动对您的本地硬盘驱动器、任何可移动媒体（如便携驱动器或光盘）和下载的内容进行扫描。你也可以设置自动扫描电子邮件。

病毒和间谍软件扫描还会检查您的计算机是否存在任何可能与恶意软件相关的更改。如果发现任何危害系统的更改（例如系统设置或更改重要系统进程的尝试），DeepGuard 会阻止该程序的运行，因为该程序很可能是恶意软件。

如何扫描我的计算机

病毒和间谍软件扫描已开启时，其将自动扫描计算机中的有害文件。您还可手动扫描文件并设置定时扫描。

建议始终开启病毒和间谍软件扫描。如需确保计算机上不存在有害文件，或要扫描已排除在实时扫描范围之外的文件，请手动扫描文件。

通过设置定时扫描，病毒和间谍软件将在特定时间删除计算机上的有害文件。

自动扫描文件

实时扫描通过扫描所有正在访问的文件和阻止访问那些包含恶意软件的文件来保护您的计算机。

计算机尝试访问某个文件时，实时扫描将扫描文件中是否存在恶意软件，而后才允许计算机访问该文件。若实时扫描发现任何有害内容，它会在文件带来任何损害前将其移至隔离区。


实时扫描是否会影响计算机的性能？

通常情况下，您不会注意到扫描进程，因为此进程耗时短且占用的系统资源少。实时扫描所需的时间和系统资源取决于文件的内容、位置和类型等。

扫描耗时较长的文件：

可移动驱动器（如 CD、DVD 和便携 USB 驱动器）上的文件。

压缩文件，如 .zip 文件。

 注意：默认情况下不会扫描压缩文件。

出现以下情况时，实时扫描可能会降低计算机速度：

您的计算机不符合系统要求，或者


您同时访问的文件过多。例如，当您打开一个包含多个待扫描文件的目录时。

开启或关闭实时扫描

让实时扫描保持开启状态，以便在恶意软件损害计算机前将其阻止。

若要开启或关闭实时扫描：

1. 在主页面上，单击 [状态](#)。
2. 单击 [更改此页面上的设置](#)。

 注意：您需要管理员权限方可关闭安全功能。


3. 开启或关闭 [病毒和间谍软件扫描](#)。
4. 单击 [关闭](#)。

自动处理有害文件

实时扫描可自动处理有害文件，而不会询问您。

若要让实时扫描自动处理有害文件：

1. 在主页上单击 [设置](#)。

 注意：您需要有管理权限才能更改设置。

2. 选择 [计算机安全 > 病毒和间谍软件扫描](#)。
3. 选择 [自动处理有害文件](#)。

若选择不自动处理有害文件，实时扫描将在发现有害文件时询问您要执行的操作。

处理间谍软件

病毒和间谍软件扫描可在间谍软件尝试启动时立即将其阻止。

在间谍软件应用程序能够启动之前，产品会将其阻止并让您决定如何处理。

发现间谍软件时选择下列操作之一：

采取的操作	针对间谍软件所采取的操作
自动处理	让产品根据所发现的间谍软件决定应采取的最佳操作。
隔离间谍软件	将间谍软件移至隔离区，使其无法损害您的计算机。
删除间谍软件	从您的计算机中删除所有与间谍软件相关的文件。
仅阻止间谍软件	阻止访问间谍软件，但让其保留在计算机中。
将间谍软件排除在扫描范围之外	允许间谍软件运行并在以后将其排除在扫描范围之外。

处理危险软件

病毒和间谍软件扫描可在危险软件尝试启动时立即将其阻止。

在危险软件应用程序能够启动之前，产品会将其阻止并让您决定如何处理。

发现危险软件时选择以下操作之一：


采取的操作	针对危险软件所采取的操作
仅阻止危险软件	阻止访问危险软件，但让其保留在计算机中。
隔离危险软件	将危险软件移至隔离区，使其无法损害您的计算机。
删除危险软件	从您的计算机中删除所有与危险软件相关的文件。
将危险软件排除在扫描范围之外	允许危险软件运行并在以后将其排除在扫描范围之外。

自动删除跟踪 Cookie

通过删除跟踪 Cookie，可阻止网站跟踪您所访问的互联网站点。

跟踪 Cookie 指允许网站记录您访问的网站的小文件。若要从计算机中删除跟踪 Cookie，请按照以下说明操作。

1. 在主页上单击 [设置](#)。

 **注意：**您需要有管理权限才能更改设置。

2. 选择 [计算机安全 > 病毒和间谍软件扫描](#)。
3. 选择 [删除跟踪 Cookie](#)。
4. 单击 [确定](#)。

手动扫描文件

您可手动扫描文件（例如，将外部设备连接至计算机时），以确保其不包含任何恶意软件。

启动手动扫描

您可扫描整个计算机，或扫描指定类型的恶意软件或指定位置。

如果怀疑有某类型的恶意软件则仅扫描这种类型。如果您怀疑计算机的某位置上有问题，则仅扫描那个部份。完成这些扫描将会比扫描整个计算机更快。

启动手动扫描计算机：

1. 在主页面上，单击**扫描**下方的箭头。
将显示扫描选项。
2. 选择扫描类型。
选择**更改扫描设置**，以优化手动扫描对计算机执行病毒和其他有害应用程序扫描的方式。
3. 如果已选择**选择要扫描的内容**，则会打开可供您选择扫描位置的窗口。
执行上述操作后，**扫描向导**会打开。

扫描类型

您可以扫描整个计算机，或扫描指定类型的恶意软件或指定位置。

以下列出了不同的扫描类型：

扫描类型	扫描对象	何时使用此扫描类型
病毒与间谍软件扫描	要进行病毒、间谍软件和危险软件扫描的计算机部分	此扫描类型比全面扫描快得多。它仅搜索系统上包含已安装程序文件的部分。如果您希望快速检查计算机是否未受感染，建议使用此扫描类型，因为它能够有效查找并删除计算机上任何活动的恶意软件。
全面计算机扫描	对您的整个计算机（内部硬盘和外部硬盘）进行扫描以查找病毒、间谍软件和危险软件	如果想完全确保计算机上无恶意软件或危险软件存在。此扫描类型耗时最长。它结合了快速恶意软件扫描和硬盘扫描。它还会检查可能由 Rootkit 隐藏的项目。
选择要扫描的内容	对特定文件、文件夹或驱动器进行扫描以查找病毒、间谍软件和危险软件	若怀疑计算机上某特定位置可能存在恶意软件，例如，该位置包含从潜在危险来源（如点对点文件共享网络）下载的内容。扫描耗时将取决于扫描目标的大小。例如，如果扫描的文件夹仅包含少数小文件，则扫描可快速完成。
Rootkit 扫描	重要系统位置上的可疑项目意味着可能存在安全问题。扫描隐藏的文件、文件夹、驱动器或进程	怀疑计算机上安装了 Rootkit 时。例如，如果最近在计算机上检测到恶意软件，并且希望确保恶意软件没有安装 Rootkit。

在 Windows 资源管理器中扫描

您可以在 Windows 资源管理器中，扫描磁盘、文件夹和文件以查找病毒、间谍软件和危险软件。

扫描磁盘、文件夹或文件：

1. 请将鼠标指针置于要扫描的磁盘、文件夹或文件上，并单击鼠标右键。

2. 通过在菜单上单击鼠标右键，选择[要进行病毒扫描的文件夹](#)。（选项名称取决于是否正在扫描磁盘、文件夹或文件。）


[扫描向导](#)窗口打开，且开始扫描。

如果发现病毒或间谍软件，[扫描向导](#)会指导您执行清除步骤。

选择要扫描的文件

在手动或定时扫描中可以选择要对其进行病毒和间谍软件扫描的文件类型。

1. 在主页上单击[设置](#)。

 注意：您需要有管理权限才能更改设置。

2. 选择[其他设置](#) > [手动扫描](#)。

3. 在[扫描选项](#)下，从以下设置中选择：

[仅扫描那些最有可能受到感染的文件类型（如可执行文件）](#)。选择此选项可加快扫描进程。将扫描有以下扩展名的文件：[.ani](#)、[.asp](#)、[.ax](#)、[.bat](#)、[.bin](#)、[.boo](#)、[.chm](#)、[.cmd](#)、[.com](#)、[.cpl](#)、[.dll](#)、[.doc](#)、[.dot](#)、[.drv](#)、[.eml](#)、[.exe](#)和[.hqx](#)。

扫描已知的文件类型

[扫描存档文件和文件夹](#)。


扫描内部压缩文件

[使用扫描时使用所有可用的启发式扫描来更好地找出新的或未知的恶意软件](#)。

 注意：如果选择此选项，则扫描会耗时较长，且会产生较多的误报结果（将无害文件报告为可疑文件）。

使用高级启发式扫描

4. 单击[确定](#)。


 注意：排除项目列表上的排除文件不会予以扫描，即使您在此选择扫描它们。

发现有害文件时应执行的操作

选择在发现有害文件时的处理方式。



若要选择手动扫描期间发现有害内容时要执行的操作：


1. 在主页上单击[设置](#)。

 注意：您需要有管理权限才能更改设置。

2. 选择[其他设置](#) > [手动扫描](#)。

3. 在[发现病毒或间谍软件时](#)中，选择以下选项：

选项	说明
询问我（默认）	您可以针对手动扫描期间发现的每个项目选择要执行的操作。
清除文件	产品将尝试自动对手动扫描期间发现的受感染文件进行杀毒。  注意：如果产品无法清除受感染文件，文件将被隔离（发现的文件位于网络或可移动驱动器上时除外），这样，文件便无法损害计算机。
隔离文件	产品会将手动扫描期间发现的任何有害文件移至隔离区，使其无法损害计算机。
删除文件	产品将删除手动扫描期间发现的任何有害文件。
仅报告	产品将不对手动扫描期间发现的任何有害文件采取任何操作，仅在扫描报告中记录检测情况。  注意：选择此选项后，若未开启实时扫描，则任何恶意软件仍能损害计算机。


 注意：若在定时扫描期间发现有害文件，其会自动清除。

计划扫描

设置在不使用计算机时自动扫描并删除病毒和其他有害应用程序，或设置定期运行扫描，以确保计算机不受感染。

计划扫描的步骤：

1. 在主页上单击[设置](#)。

 注意：您需要有管理权限才能更改设置。

2. 选择[其他设置](#) > [定时扫描](#)。

3. 开启[定时扫描](#)。

4. 选择要启动扫描的时间。

选项	描述
每日	每天扫描计算机。
每周	在每周选定日期扫描计算机。从列表中选择日期。
每月	在每月选定日期扫描计算机。若要选择日期： 1. 请选择 日期 选项。 2. 从选定日期旁的列表上选择该月的某日。

5. 选择要在选定日期开始扫描的时间。

选项	描述
开始时间	在指定时间启动扫描。

选项	描述
计算机不使用的 时间达到	在指定的一段时间内未使用计算机后启动扫描。

定时扫描在扫描计算机时使用手动扫描设置，但每次扫描存档文件并自动清除有害文件时除外。


扫描电子邮件

电子邮件扫描可保护您免遭所收电子邮件中有害文件的威胁。

必须开启病毒和间谍软件扫描，才可对电子邮件执行病毒扫描。

若要开启电子邮件扫描：

1. 在主页上单击[设置](#)。

 **注意：**您需要有管理权限才能更改设置。


2. 选择[计算机安全](#) > [病毒和间谍软件扫描](#)。
3. 选择[删除有害电子邮件附件](#)。
4. 单击[确定](#)。

何时扫描电子邮件及其附件

病毒和间谍软件扫描可删除所收到电子邮件中的有害内容。

病毒和间谍软件扫描可删除通过电子邮件程序（如 Microsoft Outlook 和 Outlook Express、Microsoft Mail 或 Mozilla Thunderbird）收到的有害电子邮件。每次电子邮件程序使用 POP3 协议从邮件服务器接收未加密的电子邮件和附件时，它便会对其进行扫描。

病毒和间谍软件扫描无法扫描 webmail（包括 Web 浏览器中运行的电子邮件应用程序，如 Hotmail、Yahoo! mail 或 Gmail）中的电子邮件。即使您未删除有害附件或使用的是 Webmail，计算机仍可防御病毒侵入。当您打开电子邮件附件时，实时扫描会在任何有害附件带来损害前将其删除。

 **注意：**实时扫描只会保护您的计算机，而不会保护您好友的计算机。仅在您打开附件时，实时扫描才会扫描附件。这意味着，如果您使用的是 Webmail 并在打开附件之前转发邮件，则可能将感染的电子邮件转发给您的好友。


查看扫描结果

病毒和间谍软件历史记录显示产品已发现的全部有害文件。

有时，产品无法在发现有害项目时执行您选定的操作。例如，如果您选择清除文件，而文件又无法清除，则产品会将其移至隔离区。您可在病毒和间谍软件历史记录中查看此信息。

若要查看历史记录：

1. 在主页上单击[设置](#)。

 **注意：**您需要有管理权限才能更改设置。

2. 选择[计算机安全](#) > [病毒和间谍软件扫描](#)。
3. 单击[查看删除历史记录](#)。

病毒和间谍软件历史记录显示以下信息：

发现有害文件的日期和时间，

恶意软件的名称及其在计算机中的位置，以及已执行的操作。

如何将文件排除在扫描范围之外

有时，您可能要将某些文件或应用程序排除在扫描范围之外。已排除项目不会接受扫描，除非将其移出排除项目列表。

- 👉 注意：实时扫描和手动扫描的排除列表是分开的。例如，如果您将某个文件排除在实时扫描范围之外，该文件在手动扫描期间依然会接受扫描，除非您也将其排除在手动扫描范围之外。

排除文件类型

若依文件类型排除文件，则不会对含有指定扩展名的文件执行有害内容扫描。

若要添加或删除想要排除的文件类型：

1. 在主页上单击[设置](#)。

👉 注意：您需要有管理权限才能更改设置。

2. 选择是否要将该文件类型排除在实时扫描或手动扫描范围之外：

选择[计算机安全](#) > [病毒和间谍软件扫描](#)，以从实时扫描中排除文件类型。

选择[其他设置](#) > [手动扫描](#)，以从手动扫描中排除文件类型。

3. 单击[将文件排除在扫描范围之外](#)。

4. 排除某一文件类型的步骤：

a) 选择[文件类型](#)选项卡。

b) 选择[排除具有这些扩展名的文件](#)。

c) 在[添加](#)按钮旁的字段中，键入要排除的文件类型的扩展名。

若要指定无扩展名的文件，请输入 "."。您可使用通配符 "?" 代表任意一个字符，或 "*" 代表任意多个字符。

例如，若要排除可执行文件，请在字段中输入 exe。

d) 单击[添加](#)。

5. 重复以上步骤以添加要从病毒扫描中排除的其他任何扩展名。

6. 单击[确定](#)以关闭[从扫描中排除](#)对话框。

7. 单击[确定](#)以应用新的设置。

选定的文件类型将排除在以后的扫描范围之外。

按位置排除文件

若依位置排除文件，则不会对指定驱动器或文件夹中的文件执行有害内容扫描。

若要添加或删除想要排除的文件位置：

1. 在主页上单击[设置](#)。

👉 注意：您需要有管理权限才能更改设置。

2. 选择是否要将该位置排除在实时扫描或手动扫描范围之外：


选择 **计算机 > 病毒和间谍软件扫描**，以将该位置排除在实时扫描范围之外。

选择 **计算机 > 手动扫描**，以将该位置排除在手动扫描范围之外。

3. 单击 **将文件排除在扫描范围之外**。

4. 排除文件、驱动器或文件夹的步骤：

- a) 选择 **对象** 选项卡。
- b) 选择 **排除对象（文件、文件夹...）**。
- c) 单击 **添加**。
- d) 选择要从病毒扫描中排除的文件、驱动器或文件夹。

 **注意：**某些驱动器可能是可移动驱动器，如 CD、DVD 或网络驱动器。无法排除网络驱动器和空白的可移动驱动器。

- e) 单击 **确定**。

5. 重复上一步骤以从病毒扫描中排除其他文件、驱动器或文件夹。

6. 单击 **确定** 以关闭 **从扫描中排除** 对话框。


7. 单击 **确定** 以应用新的设置。

选定的文件、驱动器或文件夹将排除在以后的扫描范围之外。

查看排除的应用程序

您可查看已排除在扫描范围之外的应用程序，如果您希望日后扫描该等应用程序，亦可将其从排除项目列表中删除。


如果实时扫描或手动扫描检测到某个应用程序表现得类似于间谍软件或危险软件，但您知道该应用程序是安全的，则您可将其排除在扫描范围之外，以免产品再次对此向您提出警告。

 **注意：**如果应用程序表现得类似于病毒或其他恶意软件，则无法将其排除。

您无法直接排除应用程序。新应用程序仅会在您于扫描期间将其排除时才会显示在排除列表上。

查看从扫描中排除的应用程序的步骤：

1. 在主页上单击 **设置**。

 **注意：**您需要有管理权限才能更改设置。


2. 选择是否要查看已排除在实时扫描或手动扫描范围之外的应用程序：

选择 **计算机 > 病毒和间谍软件扫描**，以查看已排除在实时扫描范围之外的应用程序。

选择 **计算机 > 手动扫描**，以查看已排除在手动扫描范围之外的应用程序。

3. 单击 **将文件排除在扫描范围之外**。

4. 选择 **应用程序** 选项卡。

 **注意：**只能排除间谍软件和危险软件应用程序，不能排除病毒。

5. 若要再次扫描已排除的应用程序：

- a) 选择要包含在扫描中的应用程序。
- b) 请单击 **删除**。

6. 单击 **确定** 以关闭 **从扫描中排除** 对话框。

7. 单击[确定](#)以退出。

如何使用隔离区

“隔离区”是用来存放可能具有恶意文件的安全区域。

隔离的文件不会传播，也不会对计算机造成任何损坏。

您可以隔离恶意软件、间谍软件和危险软件，使其不会损害计算机。必要时，您可稍后从隔离区还原某些应用程序或文件。

如果不再需要某个隔离的项目，可将其删除。从隔离区删除的项目会从计算机中永久删除。

通常，可删除所隔离的恶意软件。

在大多数情况下，可删除隔离的间谍软件。不过，隔离的间谍软件可能是合法软件程序的一部分，删除后目前的部分程序可能无法正常执行。若要将此程序保留在计算机上，可还原隔离的间谍软件。

隔离的危险软件可能为合法的软件程序。如果此程序由您自行安装及设置，则可在隔离区将其还原。如果您对危险软件的安装并不知情，则其很可能含有恶意目的，应将其删除。

查看隔离的项目

查看隔离区中项目的详细信息。

查看隔离区中项目的详细信息：

1. 在主页上单击[设置](#)。

 注意：您需要有管理权限才能更改设置。

2. 选择[计算机安全](#) > [病毒和间谍软件扫描](#)。

3. 单击[查看隔离](#)。

[隔离区](#)页面显示存储在隔离区中的项目总数。

4. 若要查看隔离区中项目的详细信息，请单击[详细信息](#)。

您可按恶意软件名称或文件路径来对内容进行排序。

系统会显示前 100 个项目的列表，包括已隔离项目的类型、名称和文件安装路径。

5. 若要查看关于已隔离项目的更多信息，请单击[状态](#)栏上项目旁的*i*图标。

还原已隔离项目

您可还原所需的已隔离项目。

如果需要，可从隔离区还原某些应用程序或文件。请勿从隔离区还原任何项目，除非您确定其不会造成任何威胁。已还原的项目返回至其在计算机上的原始位置。

还原已隔离项目

1. 在主页上单击[设置](#)。

 注意：您需要有管理权限才能更改设置。

2. 选择[计算机安全](#) > [病毒和间谍软件扫描](#)。

3. 单击[查看隔离](#)。

4. 选择要还原的隔离项目。
5. 单击[恢复](#)。

什么是 DeepGuard

DeepGuard 会分析文件内容和应用程序行为，并监视不受信任的应用程序。

DeepGuard 会阻止新的和未发现的病毒、蠕虫以及其他尝试更改计算机的有害应用程序，并防止可疑应用程序访问互联网。

如果 DeepGuard 检测到一个新应用程序尝试对系统作出具有潜在危险的更改，它将允许该应用程序在安全区域运行。在安全区域内，该应用程序不会损害您的计算机。DeepGuard 会分析该应用程序尝试作出的更改，并据此确定该应用程序为恶意软件的可能性。如果该应用程序可能是恶意软件，DeepGuard 将阻止它。

DeepGuard 检测出具有潜在危险的系统更改包括：

系统设置（如 Windows 注册表）更改，
试图关闭重要系统程序，例如类似本产品的安全程序，及
试图编辑重要的系统文件。


开启或关闭 DeepGuard

让 DeepGuard 保持开启状态，以防可疑应用程序对计算机作出具有潜在危害的系统更改。

如果您使用的是 Windows XP，确保在开启 DeepGuard 之前已安装 Service Pack 2。

若要开启或关闭 DeepGuard：

1. 在主页面上，单击[状态](#)。
2. 单击[更改此页面上的设置](#)。

 **注意：**您需要管理员权限方可关闭安全功能。

3. 开启或关闭[DeepGuard](#)。
4. 单击[关闭](#)。


允许 DeepGuard 已阻止的应用程序

您可以控制 DeepGuard 将允许和阻止哪些应用程序。

有时，即使您需要使用某应用程序并知道该应用程序是安全的，DeepGuard 可能仍然会阻止该安全应用程序的运行。出现此情况是因为该应用程序尝试作出可能具有潜在危害的系统更改。当显示 DeepGuard 弹出窗口时，您也可能会在无意中阻止该应用程序。

若要允许 DeepGuard 已阻止的应用程序：

1. 在主页上，单击[工具](#)。
2. 单击[应用程序](#)。
显示[受监视的应用程序](#)列表。
3. 找到您要允许的应用程序。

 **注意：**您可以单击列标题，以便将列表分组。例如，单击[权限](#)列，以将列表分为允许的程序组和拒绝的程序组。

4. 在权限列中选择允许。
5. 单击关闭。


DeepGuard 可再次允许应用程序作出系统更改。

在兼容模式下使用 DeepGuard

DeepGuard 会临时修改正在运行的程序，以提供最大保护。某些程序会确保自身不遭到损坏或修改，因此可能与该功能不兼容。例如，带有防诈骗工具的在线游戏会在其运行时确保不遭到任何形式的修改。此类情况下，您可开启兼容模式。

若要开启兼容模式：

1. 在主页上单击设置。

 注意：您需要有管理权限才能更改设置。

2. 选择计算机安全 > DeepGuard。
3. 选择使用兼容模式。
4. 单击确定。

如何处理可疑行为警告

DeepGuard 监视不受信任的应用程序。如果被监视的应用程序尝试访问互联网，尝试更改系统，或行为可疑，则 DeepGuard 会阻止它。

若已在 DeepGuard 设置中选择向我发出可疑行为警告，DeepGuard 将在检测到具有潜在危害的应用程序时或在您启动声誉未知的应用程序时通知您。

若要决定想要如何处理 DeepGuard 已阻止的应用程序：

1. 单击详细信息，以查看关于该程序的详细信息。

详细信息章节会显示：

应用程序的位置，
应用程序在“实时保护网络”中的声誉，以及
应用程序的通用性。

2. 决定是否信任 DeepGuard 已阻止的应用程序：

如果您不想阻止该应用程序，则选择我信任该应用程序。继续进行。。

以下情况下，应用程序很有可能是安全的：

DeepGuard 在您执行某些操作后阻止了应用程序，
您可识别该应用程序，或
您从信任的来源取得该应用程序。

如果您想要阻止该应用程序，则选择不信任该应用程序。阻止该应用程序。。

以下情况下，应用程序很有可能是不安全的：

应用程序不常见，
应用程序声誉未知，或
您不知道该应用程序。

3. 若要提交可疑应用程序以供分析：

- a) 单击[向 F-Secure 发送应用程序报告](#)。
产品将显示提交条件。
- b) 若同意条件并要提交样本，则单击[接受](#)。

建议您在以下情况下发送样本：

DeepGuard 阻止您认为是安全的应用程序，或
您怀疑该应用程序可能是恶意软件。

