SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console

策略设置指南

产品版本号： 5.5

内容

1 关于本指南

本指南说明怎样在 Sophos Enterprise Console 和 Sophos Endpoint Security and Control 软件中设置策略。

注释
您的用户授权使用许可协议中没有包括的功能，将不可用。

特别地，本指南提供建议帮助您：

- 理解策略建议。
- 按照类型设置和展开部署每个策略。
- 使用扫描选项查找项目。
- 确定从扫描中排除项目。

本指南会对您有用，如果：

- 您已在使用 Enterprise Console。
- 您需要针对策略设置和展开部署的最佳选项的建议。

在查看本指南前，请参见 Sophos Enterprise Console快速安装指南 快速安装指南。

所有 Enterprise Console 文档都可以在 http://www.sophos.com/zh-cn/support/documentation/enterprise-console.aspx 找到。

2 常规策略建议

当您安装 Enterprise Console 时，会为您创建默认的策略。这些策略会应用到您创建的任何组中。默认策略旨在提供有效的各级保护措施。如果您使用诸如网络访问控制，补丁，应用程序控制，数据控制，设备控制，或介入防范等，那么，您需要创建新的策略，或者更改默认策略。在设置策略时，请考虑：

- 尽可能地使用策略的默认设置。
- 在更改默认策略或创建新策略（例如，桌面或服务器）时，请考虑计算机的角色。
- 使用 Enterprise Console 进行所有统一的策略设置，并尽可能地在 Enterprise Console 中，而不是在计算机上设置选项。
- 只在计算机需要暂时的配置时，或者，有不能进行统一配置的项目（如：高级扫描选项）时，才在计算机本地设置选项。
- 为需要长期具有某些特殊配置的计算机，创建单独的组和策略。

3 设置更新策略

更新策略指定计算机接收新的安全隐患识别文件和 Sophos 软件的更新文件。软件预订指定从 Sophos 为各操作平台的计算机下载哪个版本的终结点软件。默认的更新策略使您能够安装和更新在“建议”软件预订中指定的软件。在设置更新策略时，请考虑：

- 您通常应该预订“建议”版本的软件，以确保它自动及时更新。不过，如果您想要在将新版本的软件部署到网络中之前，评估它们新版本，您可以会考虑在评估使用新版本时，在网络中使用“固定”版本的软件。固定的版本更新安全隐患数据，但是，不每月更新最新的软件版本。
- 请确保使用同样的更新策略的组的数量在能够管理的范围内。您从同一个路径更新的计算机通常不应该超过 1,000 台。从同一个路径中所的更新计算机的最佳数目是 600 -700 台。

  注释
  能够从同一个目录进行更新的计算机数量，取决于该目录所在的服务器，以及网络连接情况。

- 依照默认值，计算机将从单个的主路径中进行更新。不过，我们建议您同时总是设置一个进行更新的备用的副路径。如果终结点计算机无法连接到主路径，它们将尝试从副路径（如果设置了）进行更新。要了解更多信息，请参见 Sophos Enterprise Console帮助 中的 更新计算机 > 配置更新策略 部分。
- 您应该在针对进行大量漫游的笔记本电脑用户的更新策略中允许路径漫游。当启用此选项时，漫游的笔记本电脑会在它们所连接到的本地网络中，查询固定的终结点计算机，从而找到最近的路径进行更新。如果返回了多个路径，那么，笔记本电脑会确定并使用最近的那个路径。如果没有返回任何路径，那么，笔记本电脑会使用在它的更新策略中定义的主路径（然后是副路径）。

  只有漫游的笔记型电脑和固定的终结点计算机都被相同的 Enterprise Console 示例 (instance) 管理时，并且使用相同的软件预订时，路径漫游才会工作。任何第三方的防火墙，都必须被配置为允许更新路径查询和响应。默认使用的端口号为 51235，但可以更改它。

  要了解更多信息，请参见 Sophos Enterprise Console帮助 中的 更新计算机 > 配置更新策略 > 配置更新服务器 部分。有关路径漫游的常见问题，请参见 Sophos 技术支持知识库文章 112830 (http://www.sophos.com/en-us/support/knowledgebase/112830.aspx)。
- 如果您担心配置较低的计算机的运行效率，那么，您可以预订固定版本的软件，并且在您准备好为这些计算机更新软件时，手动更改软件预订。此选项将确保那些计算机更新新的安全隐患检测数据。或者，您为配置较低的计算机进行次数较少的更新（例如：每天 2-3 次），或者，考虑在用户不繁忙的时间进行更新（例如：在晚间或周末）。

  警告
  请意识到缩减更新次数会增加计算机的安全风险。

4 设置防病毒和 HIPS 策略

4.1 建议的设置

防病毒和 HIPS 策略 指定安全软件怎样扫描计算机中的病毒、木马、蠕虫、间谍软件、广告软件、可能不需要的应用程序 (PUA)、可疑行为和可疑文件；以及怎样清除它们。在设置防病毒和 HIPS 策略时，请考虑：

- 默认的防病毒和 HIPS 策略，将保护计算机免遭病毒和其它恶意软件的侵害。不过，您可能还想要创建新的策略，或更改默认策略，以便能够检测其它可能不需要的应用程序或行为。
- 为了充分利用默认情况下已经启用的 Sophos Live Protection 的优点，我们还建议选中向 Sophos 自动发送样本文件选项。
- 启用恶意数据流检测，它可以检测僵尸网络或其他恶意软件攻击中涉及的端点计算机和命令与控制服务器之间的通信。默认情况下，新安装的 Enterprise Console 5.3 或之后版本会启用检测恶意数据流选项。如果已从之前版本的 Enterprise Console 升级，则需要启用此选项以使用该功能。

  注释
  恶意数据流检测目前仅在 Windows 7 及更高版本的非服务器操作系统上得到支持。它需要 Sophos Live Protection。

- 使用仅限警报 选项，可以仅限于检测可疑行为。在开始时，定义一个“仅限报告”策略，可以使您较好地查看网络中的可疑行为的情况。此选项默认为启用，一旦策略的展开部署完成后，就应该取消选中它，以便能够阻断程序和文件。

有关详细信息，请参阅 Sophos 技术支持知识库文章 114345 (http://www.sophos.com/en-us/support/knowledgebase/114345.aspx)。

4.2 怎样展开部署防病毒和 HIPS 策略

我们建议您按照以下说明展开部署防病毒和 HIPS 策略：

1. 为不同的组创建不同的策略。
2. 设置 Sophos Live Protection 选项。此功能使用 Sophos 在线查找服务，立即确定某可疑文件是否为安全隐患，并实时更新您的 Sophos 软件，提供最及时的安全隐患防范。恶意数据流检测和下载信誉功能需要 Sophos Live Protection。
   - 请确保选中了启用 Live Protection 的读写扫描功能和启用 Live Protection 的即时扫描功能选项。如果在某个端点计算机上进行的防病毒扫描已确定某个文件可疑，但是无法根据存储在计算机上的安全隐患识别文件 (IDE)，进一步识别它是无害的，还是恶意的，那么，该文件的某些特征（如：检查和，以及其它属性）就会被发送给 Sophos，进行进一步分析。Sophos 在线查找服务在 SophosLabs 数据库中进行对可疑文件的快速查找。如果该文件被确定为有害的，或无害的，此信息会被发送回计算机，并且此文件的状态会被自动更新。
   - 选中向 Sophos 自动发送样本文件选项。如果某个文件几乎肯定就是恶意的，但是却无法只根据文件特征来确定为恶意的，那么，Sophos Live Protection 会允许 Sophos 要求该文件的样本。启用 Live Protection 后，如果启用“向 Sophos 自动发送样本文件”选项，而 Sophos 尚未拥有该文件的样本，该文件将会自动提交。提交这样的文件样本，可以帮助 Sophos 不断提高检测恶意软件，减少误报的能力。

重要提示
您必须确保文件数据将要发送到的 Sophos 域名，在您的网络筛选方案中是受信任的网站域名。要了解详情，请参见 Sophos 技术支持知识库文章 62637 (http://www.sophos.com/en-us/support/knowledgebase/62637.aspx)。如果您使用 Sophos 的网络筛选解决方案，如 WS1000 Web Appliance，则不需要再做什么。Sophos 域名已被设置为受信任。

3. 检测病毒和间谍软件。
   a) 确保启用读写扫描，或者计划完整系统扫描检测病毒和间谍软件。读写扫描在默认情况下是启用的。有关详细信息，请参阅使用读写扫描 （第 26 页）或使用计划扫描 （第 27 页）。
   b) 为病毒/间谍软件选择清除选项。
4. 检测可疑文件。
   可疑文件中包含某些恶意软件所共有的特征，但是这些特征还不足以确定这些文件为新出现的恶意软件。
   a) 启用读写扫描，或者计划完整系统扫描检测可疑文件。
   b) 在扫描设置中，选中可疑文件选项。
   c) 对可疑文件选择清除选项。
   d) 根据需要，批准将要允许运行的文件。
5. 检测恶意和可疑行为、缓冲区溢出以及恶意数据流（行为监控）。
   这些选项可以不断监控正在运行的进程，以确定程序在运行中是否出现恶意或可疑的行为。它们有助于中止安全隐患。
   a) 确保启用了读写扫描的行为监控。默认情况下它是启用的。
   b) 确保选中检测恶意数据流选项。
   c) 使用仅限警报选项，可以仅检测可疑行为和缓冲区溢出。此选项在默认情况下是启用的。
   d) 批准您想在今后继续运行的任何程序或文件。
   e) 清除仅限警报选项，可以配置您的策略阻断检测到的程序和文件。
   此方法可以避免阻断用户可能需要的程序和文件。有关详细信息，请参阅 Sophos 技术支持知识库文章 50160 (http://www.sophos.com/en-us/support/knowledgebase/50160.aspx)。
6. 检测广告软件和可能不需要的应用程序。
   当您首次扫描广告软件和可能不需要的应用程序时，此扫描可能会生成大量有关已经在您的网络运行的应用程序的警报。通过最初运行计划扫描的办法，您可以妥当处理已经在网络中运行的应用程序。
   a) 计划一次完整系统扫描，以检测所有的广告软件和可能不需要的应用程序。
   b) 批准或卸载此扫描检测到的程序。
   c) 选中广告软件和可能不需要的应用程序读写扫描选项，可以检测广告软件和可能不需要的应用程序。
   有关详细信息，请参阅 Sophos 技术支持知识库文章 13815 (http://www.sophos.com/en-us/support/knowledgebase/13815.aspx)。
7. 检测网页中的安全隐患。
   此选项会阻断已知的含有恶意代码的网站，并且会扫描下载的内容中是否有恶意代码，帮助您防范恶意软件。
   a) 请确保阻断访问恶意网站选项设置为开启，以阻断恶意网站。此选项在默认情况下是开启的。
   b) 将内容扫描选项设置为开启或当读写时，可以扫描和阻止下载的恶意数据。仅当读写扫描启用时，默认的设置当读写时才会启用下载扫描。

c) 根据需要，批准所有允许的网站。

d) 确保启用了文件信誉检查。

注释
此外，您还可以使用 Web 控制策略，筛选前 14 个最不合适的网站类别，从而控制用户网络访问。有关如何设置 Web 控制策略的信息，请参阅建议的设置 （第 22 页）。

有关设置防病毒和 HIPS 策略的详细信息，请参阅 Sophos Enterprise Console帮助。

5 设置防火墙策略

5.1 关于防火墙策略

防火墙策略指定防火墙怎样保护计算机。只有经过批准的应用程序，或某类应用程序才能被允许访问公司网络或因特网。

注释
Sophos Client Firewall 在服务器版的操作系统上不被支持。要了解有关硬件和操作系统的要求，请参见 Sophos 网站（http://www.sophos.com/zh-cn/products/all-system-requirements）中的系统要求页面。

警告
您必须在使用之前先配置防火墙策略。通过 Sophos Enterprise Console 将没有配置过的默认策略部署到计算机中，会引起网络通讯问题。

默认的策略并不是用于“直接”部署的，它不能满足通常的使用需要。默认策略只是为您配置自己的策略提供一个基础。

依照默认值，防火墙会被启用，阻断所有可有可无的连接。任何超出基本网络连接范围的东西，例如，您的电子邮件软件，网页浏览器，以及任何网络数据库访问，都会不会在默认策略下正常工作，因为，默认策略会阻断所有不是最根本的网络连接。因此，您应该配置它允许您想使用的通讯流，应用程序，以及进程，并在安装防火墙到所有的计算机上之前，测试它。

5.2 规划防火墙策略

在创建或编辑防火墙规则（全局，应用程序，或其它）之前，请规划您的防火墙策略，以及您预想它们做什么。

在规划您的防火墙策略时，您应该考虑：

- 那些计算机应该安装 Sophos Client Firewall。
- 该计算机是台式机还是笔记本电脑。您可能会想为笔记型电脑设置双重路径。
- 您想要使用哪种路径检测方法，即：DNS 查找，还是网关 MAC 地址检测。
- 网络的支持系统和协议
- 远程连接

根据涉及的各种应用程序和不同的用户组所需要的网络访问权限，决定需要创建多少防火墙策略。这些策略将涉及不同的策略，并且具有各种不同的限制。请记住，多策略要求在 Enterprise Console 在中具有多个组。

- 您不应该只使用一个 Sophos Client Firewall 策略。您只会被强制在一台或两台计算机（如：管理员的工作站计算机）上添加规则，但是这些规则会被应用到整个网络中。这存在着安全风险。
- 相反地，大量使用各种配置，则意味着更多的时间要花费在监控和维护上。

网络的支持系统和协议

考虑您的网络所依赖的各种服务。例如：

- DHCP
- DNS
- RIP
- NTP
- GRE

默认的防火墙配置中的规则将管理这些服务中的大多数。不过，留意哪些是您应该允许的服务，那些是您不需要的服务。

远程访问计算机

如果您要使用远程访问软件监控和修复计算机，那么，您必须在配置中设定规则，使得这项任务可以进行。

识别您访问联网计算机时，所采用的技术手段。例如：

- RDP
- VPN 客户端/服务器
- SSH/SCP
- Terminal 服务
- Citrix

检查需要哪种访问，并创建相应的规则。

5.3 建议的设置

在设置您的防火墙策略时，请考虑：

- 在 Sophos Client Firewall 安装了之后，Windows Firewall 会关闭。因此，如果您过去使用的是 Windows Firewall，请记下现有的配置，并将它们移至 Sophos Client Firewall。
- 使用 默认允许 模式，以检测但不阻断通讯流，应用程序，以及进程。在开始时，定义一个“仅限报告”策略，可以使您较好地查看网络活动的情况。
- 使用防火墙“事件查看器”，查看在使用哪些通讯流，应用程序，和进程。“事件查看器” 还允许您轻松创建规则，允许或阻断报告的通讯流，应用程序，以及进程。单击 事件 > 防火墙事件，您可以访问“事件查看器”。
- 通过“事件查看器”查看所创建的规则。一个应用程序可能会引发多个防火墙事件 — 同一个应用程序的不同操作引发不同的事件 — 但是一个应用程序规则必须覆盖全部应用程序措施。例如，某个电子邮件客户端应用程序在发出电子邮件和接收电子邮件时，可能引发两个不同的事件，但是，针对该客户端应用程序的应用程序规则必须能够处置这两种操作。
- 允许使用网页浏览器，电子邮件，文件和打印机共享。
- 我们建议您不要更改默认的 ICMP 设置，全局规则，以及应用程序规则，除非您具备联网技术知识。
- 我们建议您尽可能创建应用程序规则，而非全局规则。

- 不要在设置了双路径的策略中使用 交互 模式。
- 不要在大型或中型的网络中，以及域环境中使用 交互 模式。在非常小的网络中（如：不超过 10 台计算机）的工作组环境中，以及在独立使用的计算机上，可以使用 交互 模式创建防火墙规则。

5.4 配置防火墙双重路径

单一路径选项，供总是在单一的网络中的计算机（如：台式机）使用。如果您想要防火墙根据计算机所在的路径（如：在办公室内，或在办公室外。）来使用不同的设置，那么，可以选择双重路径选项。您可能会为笔记型电脑设置双重路径。

如果您选择双重路径，我们建议您按照以下说明，设置主路径和副路径配置选项：

- 设置主路径为您控制的网络（如：办公网络），而副路径为您不能控制的路径。
- 设置对主路径的访问权限较为开放，而对副路径的访问权限较为严格。
- 在配置主路径的检测选项时，我们原则上建议对于大规模的，复杂网络使用 DNS 检测，而对于小规模的，简单网络使用网关检测。DNS 检测要求 DNS 服务器，但是它通常比网关检测易于维护。如果用于网关检测的硬件失灵，那么，必须重新配置 MAC 地址；在硬件重新配置完成之前，计算机可能会错误地接收到副路径的设置。
- 如果您使用 DNS 检测，我们建议您添加特定的 DNS 条目到您的 DNS 服务器，使该服务器具有特异名，并且返回本地主机 IP 地址，该地址也称为环回地址 (loopback address)（即：127.x.x.x）。这些选项使您连接的其它网络几乎完全不可能被错误地检测为您的主网络。
- 在高级防火墙策略配置的 常规 标签页的 应用的路径 部分，选择您想要应用到计算机的防火墙配置。如果您想要根据计算机所在的路径决定所应用的配置，请选择 应用针对检测到的路径的配置选项。如果您想要手动应用主路径配置或副路径配置，请选择相应的选项。

警告
我们强烈建议谨慎使用本地子网规则作为副路径配置的一部分。如果是在办公地点之外使用的笔记本电脑，那么，它可能会连接到未知的子网中。如果出现这种情况，那么，使用了本地子网作为地址的副路径设置中的防火墙规则，可能会无意中允许未知的通讯流。

5.5 怎样展开部署防火墙策略

部署使您能够监控网络中的所有通讯流的策略。您会在“防火墙事件查看器”中收到通讯流报告。使用这些信息来设置基本的策略。

您应该分阶段地在网络中展开部署 Sophos Client Firewall，即一次展开部署 Sophos Client Firewall 到一个计算机组中。这将避免在初始阶段造成网络中涌现大量通讯流。

警告
在配置被彻底检查和测试之前，不要在整个网络中部署。

1. 将 Sophos Client Firewall 部署到供测试的计算机组中，这些计算机组应该体现联网计算机的各种不同的角色。
2. 配置防火墙策略使用 默认允许 模式，检测但并不阻断常用的通讯流，应用程序和进程，并将策略指派到供测试的计算机组中。

   a) 创建新的防火墙策略。在 Enterprise Console 的 策略 窗格板中，右击 防火墙 和选择 创建策略。命名此策略，然后双击它。
   会出现 防火墙策略 向导。

b) 单击 下一步 以使用向导配置策略，或者，单击 高级防火墙策略 以手动方式配置策略。

- 使用向导：单击 下一步。选择 单一路径 并单击 下一步。选择 监控，单击 下一步，然后再单击 下一步，然后单击 完成。
- 使用 高级防火墙策略 选项：在 防火墙策略 对话框中的 主路径 旁，单击 配置。在 常规 标签页中，将工作模式设置为 默认为允许。单击 确定，然后再次单击 确定。

c) 将新建的防火墙策略指派给供测试的计算机组。

3. 使用“防火墙事件查看器”，查看在使用哪些通讯流，应用程序，和进程。“事件查看器” 还允许您轻松创建规则，允许或阻断报告的通讯流，应用程序，以及进程。单击 事件 > 防火墙事件，您可以访问“事件查看器”。
4. 在一段时间内（如：数星期）监控防火墙事件，并逐步完善防火墙策略。

   a) 从“事件查看器”中创建规则。右击某个事件为它创建规则。有关创建防火墙规则的详细信息，请参阅 Sophos Enterprise Console帮助，配置策略 > 防火墙策略部分。

   b) 检查策略中是否有任何缺点（例如：某些用户具有过多的访问权限）。

   c) 在需要有所不同时，请在组中划分出子组，并创建额外的策略和规则。
5. 通过“事件查看器”查看所创建的规则。一个应用程序可能会引发多个防火墙事件 — 同一个应用程序的不同操作引发不同的事件 — 但是一个应用程序规则必须覆盖全部应用程序措施。例如，某个电子邮件客户端应用程序在发出电子邮件和接收电子邮件时，可能引发两个不同的事件，但是，针对该客户端应用程序的应用程序规则必须能够处置这两种操作。
6. 将您的网络分成不同的计算机，分别体现出网络中不同的角色，例如，销售工作站，IT 管理员工作站，等等。
7. 一旦您感到已涵盖了方方面面，比如，您不再收到许多没有规则处理的新防火墙事件，那么，您就可以将您的规则创建为各种策略，并根据需要指派它们。如果您的网络中的计算机数量很多，那么，我们建议您一次部署 Sophos Client Firewall 到一个计算机组。
8. 一旦您检测了规则，请更改策略模式为 默认为阻断；否则，计算机会处于不安全的状态。

有关设置防火墙策略的详细信息，请参阅 Sophos Enterprise Console帮助，配置策略 > 防火墙策略部分。

注释

如果要在非常小的网络中，或者在运行 Windows 7 或更早版本的单个独立用户的计算机上，使用“防火墙事件查看器”监控网络通讯流和创建规则，您可以在供测试的计算机上安装 Sophos Client Firewall，并在交互模式中配置它。仅可能多地运行您的网络中的各种应用程序，包括运行各种网页浏览器。然后，导入和编辑包含了在这一使用过程中建立的各种规则的防火墙配置。要了解更多的信息，请参见 Sophos Endpoint Security and Control帮助。

6 设置应用程序控制策略

6.1 建议的设置

应用程序控制 策略指定在您的计算机上阻断哪些应用程序，允许哪些应用程序。在设置您的应用程序控制策略时，请考虑：

- 使用 检测但允许运行 选项，检测但不阻断受控应用程序。在开始时，定义一个“仅限报告”策略，可以使您较好地查看网络中的应用程序使用情况。
- 使用应用程序控制“事件查看器”以审查公司内的应用程序使用情况。单击 事件 > 应用程序控制事件，您可以访问“事件查看器”
- 使用“报告管理器”，创建有关按照计算机或用户区分的应用程序控制事件的趋势报告。
- 考虑使用 “将来全部由 Sophos 添加” 选项，阻断所有 Sophos 添加的特定类型的新的应用程序，这样您就不必总是要更新您的策略。例如，如果您当前阻断了所有的即时消息(instant messaging)应用程序，您可能同样要阻断所有新出现的即时消息(instant messaging)应用程序。

6.2 怎样展开部署应用程序控制策略

依照默认值，所有的应用程序和应用程序类型都会被允许。我们建议您按照以下说明采用应用程序控制的功能：

1. 确定您想要控制的应用程序。
2. 启用读写扫描，并勾选 检测但允许运行 选项，以检测但并不阻断受控程序。
   在这之后，您将具有针对整个网络的一个应用程序控制策略。
3. 使用应用程序控制“事件查看器”，查看在使用哪些应用程序，并确定您想要阻断的应用程序，或应用程序类型。单击 事件 > 应用程序控制事件，您可以访问“事件查看器”
4. 要使不同的计算机组能够访问的应用程序不同，请为不同的组创建不同的策略。例如：您可能不想允许在办公室中的台式机上使用语音 IP 电话，但您可能想允许在远程计算机上使用它。
5. 确定您想要阻断的应用程序或应用程序类型，并将它们移至“已阻断”列表中。
6. 取消勾选 检测但允许运行 选项，可以配置您的策略阻断检测到的受控程序。

使用这种方式，您可以避免触发大量的警报，以及阻断用户可能需要的应用程序。要了解更多有关设置应用程序控制策略的信息，请参见 Sophos Enterprise Console帮助。

注释
“应用程序控制”可以被配置为阻断补丁所使用的 CScript.exe 文件。如果您同时使用“应用程序控制”和“补丁”，那么，请确保不要阻断 编程/脚本工具 类别中的 Microsoft WSH CScript。依照默认值，编程和脚本工具是被允许的。

7 设置数据控制策略

7.1 定义数据控制策略

数据控制策略使您能够管理从计算机上不慎传输出敏感数据的风险。

各个公司都会有它自己的有关敏感数据的定义。常见的例子包括：

- 包含个人识别信息的客户记录。
- 如信用卡号码之类的财务信息。
- 机密文档。

当数据控制策略启用时，Sophos 会在通常的数据输出点监控用户的操作：

- 传输文件到存储设备（可移动存储设备，光学介质，以及磁盘介质）。
- 上传文件到应用程序（公司网页浏览器，电子邮件客户端，以及即时消息客户端）。

数据控制规则由三个要素组成：

- 匹配条件：选项包括文件内容，文件类型，以及文件名称。
- 监控要点：监控要点包括存储设备类型和应用程序。
- 采用措施：可用的措施包括“允许文件传输和日志事件”（监控模式），“允许用户接受的传输和日志事件”（学习模式），以及“阻断传输和日志事件”（限制模式）。

例如，可以定义数据控制规则记录使用 IE 浏览器上传的任何电子表格，或者，经用户确认后，允许将客户的地址传输到 DVD 盘上。

根据内容来定义敏感数据，可能会是件复杂的事情。Sophos 提供预置的敏感数据定义库，即：内容控制列表 (CCL)，来简化这一任务。该库覆盖了范围广泛的个人识别信息格式和财务信息格式，并且由 Sophos 及时更新。如果需要，您还可以自定义内容控制列表 (CCL)。

与所有的 Sophos 策略一样，数据控制策略会不断被强制实施到计算机上，即使在计算机与公司网络断开连接时，也是如此。

7.2 建议的设置

在设置您的数据控制策略时，请考虑：

- 使用 允许文件传输和日志事件 措施，检测但不阻断受控数据。在开始时，定义一个“仅限报告”策略，可以使您较好地查看网络中的数据使用情况。
- 使用 允许用户接受的传输和日志事件 措施，以提醒用户传输可能包含了敏感数据的文档的风险。此方法可以降低数据丢失的风险，同时不会对 IT 的运行效率造成显著的影响。
- 使用内容规则中的“数量”设置，配置触发警报之前相应的规则所允许的敏感数据的数量。例如：某配置为在文档中查找一个邮寄地址的规则，会比某查找 50 个或更多的地址的规则，要生成更多的数据控制事件。

> 注释
> Sophos 会为各个内容控制列表 (CCL) 提供默认的数量设置。

- 使用数据控制“事件查看器”可以快速过滤要仔细查看的事件。所有的数据控制事件和措施，都会统一记录在 Enterprise Console 中。单击 事件 > 数据控制事件，您可以访问“事件查看器”
- 使用“报告管理器”，创建有关按照规则，计算机，或用户区分的数据控制事件的趋势报告。
- 使用自定义桌面消息发送选项，向用户提供措施被触发时的额外的指导准则。例如，您可以提供说明公司的数据安全制度的链接。
- 使用详尽日志记录模式，可以收集有关数据控制规则的准确性的更多的详情。一旦完成对这些规则的评估，请禁用详尽日志记录模式。

注释
详尽日志记录模式必须在各台计算机上逐一启用。所有生成的数据都存储在计算机的本地数据控制日志中。当详尽日志记录模式处于启用状态时，每个文件中的所有匹配规则中指定的数据的字符串，都会被记录到日志中。日志的额外的详细信息，可以用来识别文档中触发了事件控制日志的短语或字符串。

7.3 怎样展开部署数据控制策略

依照默认值，数据控制是关闭的，并且没有指定任何规则监控或限制向存储设备，或向应用程序进行的文件传输。我们建议您按照以下说明采用数据控制的功能：

1. 了解数据控制是怎样在计算机上工作的：
   - 存储设备：数据控制会介入分析通过“资源管理器”（包括 Windows 桌面）复制到受控的存储设备的所有文件。不过，直接在应用程序（如：Microsoft Word）内部进行的复制，或者，使用命令行提示窗进行的传输，不会被介入分析。

     通过“允许用户接受的传输和日志事件”措施，或“阻断传输和日志事件”措施，可以强制只能使用“资源管理器”将所有的传输复制到受监控的存储设备中。在这两种情况中，任何试图直接从应用程序中保存文件，或者，从命令行提示窗中传输文件的操作，都会被数据控制阻断，并且会显示桌面警报，要求用户使用“资源管理器”进行文件传输。

     如果数据控制策略中只包含“阻断传输和日志事件”措施的规则，那么，直接从应用程序中保存文件，或者，从命令行提示窗中传输文件，将不会被介入。这样将使用户能够不受限制地使用存储设备。不过，数据控制事件仍然只日志记录使用“资源管理器”进行的传输。

     注释
     此限制不应用于应用程序监控。

   - 应用程序：数据控制介入上传到受监控的应用程序中的文件和文档。为了确保只监控用户上传的文件，某些系统文件所在的路径会从数据控制监控中排除。要了解更多有关应用程序中扫描或不扫描的内容或措施的信息，请参见 了解应用程序中的数据控制扫描 （第 14 页）。

     注释
     如果您监控电子邮件客户端，数据控制将扫描所有的文件附件，但是不会扫描电子邮件的内容。如果需要扫描电子邮件内容，可以使用 Sophos Email Security and Data Protection 解决方案。

2. 确定您想要识别的并为其创建规则的信息类型。Sophos 提供了一组样本规则，可以用来帮助设置您的数据控制策略。

重要提示
内容扫描可能会是工作量很大的过程，在创建内容规则时应该考虑这一点。很重要的是，要在将内容规则展开部署到大量的计算机上之前，测试该内容规则的影响。

注释
在您首次创建策略时，我们建议您专门针对文件中大规模收集个人识别信息的内容。Sophos 提供了样本规则，以满足此要求。

3. 启用数据控制扫描，并在您的规则中选择 允许文件传输和日志事件 措施，以检测但不阻断受控数据。

重要提示
我们建议您在初始部署时，配置所有的规则使用此措施。这将使您能够在不影响用户工作的情况下，评估规则的效率。

4. 部署您的数据控制策略到数量不多的计算机上，将易于分析由策略触发的数据控制事件。
5. 使用数据控制“事件查看器”，查看被使用的数据，检查所测试的配置中是否有缺点（例如，某规则太敏感，生成数量大大超过预期的事件。）单击 事件 > 数据控制事件，您可以访问“事件查看器”
6. 一旦测试了策略，您可以对其进行任何调整，并将其部署到数量更多的计算机上。在此阶段，您可能决定要：
   - 根据 允许用户接受的传输和日志事件 或 阻断传输和日志事件 的需要，更改某些规则的措施。
   - 为不同的组创建不同的策略。例如，您可能会允许人事部门的计算机访问个人识别信息，但是阻断所有其它组中的计算机对此的访问。

要了解更多有关设置数据控制策略的信息，请参见 Sophos Enterprise Console帮助。

7.4 了解应用程序中的数据控制扫描

以下是在所支持的应用程序中扫描或不扫描的内容或措施的列表。

要了解数据控制的已知限制的完整列表，请参见 Sophos 技术支持知识库文章 63016 (http://www.sophos.com/en-us/support/knowledgebase/63016.aspx)。

应用程序	数据控制扫描措施
网页浏览器	扫描 • 上传文件 • Webmail 附件 • Microsoft SharePoint 上传文件 不扫描 • Webmail 邮件内容 • 博客条目 • 下载文件 注释 在少数情况下，有可能扫描下载文件。
电子邮件客户端	扫描 • 电子邮件附件 不扫描 • 电子邮件内容 • 转发附件 • 在应用程序（如：资源管理器和 Microsoft Office）中，使用“发送”电子邮件选项发出的附件。 • 在“资源管理器”中使用“以电子邮件形式发送此文件”选项发送的附件。 • 从某电子邮件中复制到另一个电子邮件中的附件。 • 保存的附件。 注释 在少数情况下，有可能扫描保存的文件。
即时消息 (IM) 客户端	扫描 • 文件传输 注释 同一文件可能被扫描两次：一次是在上传到 IM 客户端时，再次是在收件人接收时。两次扫描均发生在寄件人的计算机上。 不扫描 • IM 消息内容 • 发出的文件

8 设置设备控制策略

8.1 建议的设置

设备控制策略指定批准哪些存储设备和网络设备可以用于计算机上。在设置您的设备控制策略时，请考虑：

- 使用 检测但不阻断设备 选项，可以检测但不阻断受控设备。要这样做，您必须首先将您想要检测的各个设备类型的状态设置为 已阻断。此软件不会扫描任何您尚未指定的设备类型。在开始时，定义一个“仅限报告”策略，可以使您较好地查看网络中的设备使用情况。
- 使用设备控制“事件查看器”可以快速过滤要仔细查看的阻断事件。单击 事件 > 设备控制事件，您可以访问“事件查看器”
- 使用“报告管理器”，创建有关按照计算机或用户区分的设备控制事件的趋势报告。
- 考虑对于可以访问敏感信息的计算机的用户提供较严的访问控制。
- 在展开部署阻断设备的策略之前，规划一份设备免除列表。例如，您可能会允许在从事艺术工作的计算机上使用光驱。
- “安全的可移动存储设备”分类，可以用来自动批准所支持的各种硬件加密 USB 存储设备。在 Sophos 网站中可以查看所支持的生产商的列表。要了解所支持的安全移动存储设备的列表，请参见 Sophos 技术支持知识库文章 63102 (http://www.sophos.com/en-us/support/knowledgebase/63102.aspx)。
- 当添加设备免除到设备控制策略时，请在 说明 栏中说明免除设备的理由，和提出免除设备的人员。
- 使用自定义的桌面消息发送选项，向用户提供发现受控设备时的额外的指导准则。例如，您可以提供说明公司的设备使用制度的链接。
- 如果您想要在计算机与网络断开物理连接时，启用无线网络设备（即：Wi-Fi 适配器），请在为网络设备设置访问级别时，选择 阻断桥接 选项。

  注释
  “阻断桥接模式”可以显著地降低在公司网络和非公司网络之间的网络桥接风险。此模式可用于无线和调制解调类型的设备。此模式的工作方式为，当某终结点计算机（通常是通过以太网连接的方式）连接到物理网络时，则禁用无线或调制解调网络适配器。一旦终结点计算机与物理网络断开了连接，无线或调制解调网络适配器会顺畅地重新启用。

- 确保您在展开部署策略之前，对于要阻断的设备有确切的把握。请考虑所有用户的具体情况，特别是与 WiFi 和网络设备有关的用户。

  警告
  策略的更改是在网络中通过 Enterprise Console 服务器向计算机进行的；因此，一旦网络被阻断，它就无法从 Enterprise Console 解除阻断，因为计算机将无法接收到来自服务器的添加的配置。

8.2 怎样展开部署设备控制策略

依照默认值，设备控制是关闭的，所有的设备都会被允许。我们建议您按照以下说明采用设备控制的功能：

1. 确定您想要控制的设备。
2. 启用设备控制扫描，并选择 检测但不阻断设备 选项，以检测但并不阻断受控设备。要这样做，您必须首先将您想要检测的各个设备类型的状态设置为 已阻断。此软件不会扫描任何您尚未指定的设备类型。

   在这之后，您将具有针对整个网络的一个设备控制策略。
3. 使用设备控制“事件查看器”，查看在使用哪些设备，并确定您想要阻断的设备，或设备类型。单击 事件 > 设备控制事件，您可以访问“事件查看器”
4. 要使不同的计算机组能够访问的设备不同，请为不同的组创建不同的策略。例如，您可能不想允许人事部门和财务部门使用可移动存储设备，但是，允许 IT 部门和销售部门使用它们。
5. 免除您不想阻断的具体设备或设备型号类型。例如，您可以免除某个特定的 USB 盘（具体设备）或所有的 Vodafone 3G 调制解调器（型号类型）。
6. 确定您想要阻断的设备，并将它们的状态更改为 已阻断。您还可以只允许对某些存储设备进行读访问。
7. 取消勾选 检测但不阻断设备 选项，可以配置您的策略阻断受控设备。

使用这种方式，您可以避免触发大量的警报，以及阻断用户可能需要的设备。要了解更多有关设置设备控制策略的信息，请参见 Sophos Enterprise Console帮助。

9 设置介入防范策略

9.1 关于介入防范策略

介入防范功能使您能够防范已知的恶意软件，以及防止用户（技术知识不足的本地管理员）重新配置，卸载或禁用 Sophos 安全软件。不知道介入防范的密码的用户，将不能执行这些操作。

注释
介入防范不针对具备丰富的计算机技术知识的用户。它无法防范专门瓦解操作系统的检测功能的恶意软件。此类的软件只能通过对安全隐患和可疑行为的扫描，才能被发现。要了解更多信息，请参见建议的设置 （第 4 页）。

启用防篡改保护并创建防篡改保护密码后，不知道密码的用户将不能在 Sophos Endpoint Security and Control 中重新配置读写扫描或可疑行为检测，不能禁用防篡改保护功能，也不能从“控制面板”中卸载 Sophos Endpoint Security and Control 组件（如 Sophos Anti-Virus、Sophos Client Firewall、Sophos AutoUpdate 或 Sophos Remote Management System）。

在设置您的介入防范策略时，请考虑：

- 使用介入防范“事件查看器”，核实介入防范密码的使用情况，以及监控发生介入尝试的频率。您可以查看成功的介入防范认证事件（经授权的用户越过介入防范），以及失败的尝试介入 Sophos 安全软件。单击 事件 > 介入防范事件，您可以访问“事件查看器”。

9.2 关于增强的防篡改保护

增强的防篡改保护以防篡改保护功能为基础。如果启用增强的防篡改保护，将阻止 Sophos Anti-Virus、Sophos AutoUpdate、Sophos Management Communication System、Sophos Remote Management System 和 Sophos Endpoint Defense 的以下操作：

- 从服务用户界面停止服务
- 从任务管理器用户界面停止服务
- 从服务用户界面修改服务配置
- 从命令行停止服务/编辑服务配置
- 卸载
- 重新安装
- 从任务管理器用户界面停止进程（如有必要）
- 删除或修改受保护的文件或文件夹
- 删除或修改受保护的注册表项

重要提示
要启用增强的防篡改保护，必须启用防篡改保护。

9.3 怎样展开部署介入防范策略

依照默认值，介入防范是禁用的。我们建议您按照以下说明采用介入防范策略的功能：

注释
如果您在安装过程中启用增强的防篡改保护，将会启用防篡改保护。

1. 启用介入防范，并创建安全的介入防范密码。
   此密码只允许经授权的终结点用户重新配置，禁用，或卸载 Sophos 安全软件。

   注释
   介入防范不会影响 SophosUser 和 SophosPowerUser 组中的成员。当介入防范启用后，这些用户仍然能够执行它们平常经过授权而可以执行的所有任务，并不需要输入介入防范密码。

2. 如果您要求针对不同的组，能够启用或禁用介入防范，或者，创建不同的密码，那么，请为不同的组创建不同的策略。

   重要提示
   如果禁用防篡改保护，将自动禁用增强的防篡改保护。

要了解更多有关设置介入防范策略的信息，请参见 Sophos Enterprise Console帮助。

10 设置补丁策略

10.1 关于补丁策略

补丁策略使您能够检查计算机是否安装了及时更新的安全补丁。

SophosLabs 提供的评级可以帮助您了解最重要的安全补丁问题，以便您能够迅速解决它们。SophosLabs 的评级将考虑最新的安全实例，因此该评级可能与软件商提供的严重性级别不同。

设置您的补丁策略时，请考虑使用补丁评估事件查看器审核您公司计算机上缺失的补丁。它提供有关安全补丁和补丁评估结果的信息。在补丁策略中启用了补丁评估后，您可以按照计算机，计算机组，或安全隐患等分类来查看补丁状态。单击 查看 > 补丁评估事件，您可以访问“事件查看器”。

注释
补丁使用的 CScript.exe 文件会被“应用程序控制”阻断。如果您同时使用“应用程序控制”和“补丁”，那么，请确保不要阻断 应用程序控制 策略中 编程/脚本工具 类别中的 Microsoft WSH CScript。依照默认值，“应用程序控制”不允许编程和脚本工具。

10.2 怎样展开部署补丁策略

最初，“默认的 ” 补丁策略将应用于所有的计算机。“补丁评估”在默认策略中是禁用的。

一旦启用了补丁评估，计算机立即就会进行一次评估。这会花费几分钟的时间。以后的评估则按照在策略中设定的频率进行，它的默认值为每天一次。

注释
如果计算机在 Enterprise Console 首次从 Sophos 下载补丁数据之前，就进行评估，那么，“补丁事件”查看器中不会显示任何结果。下载可能会花费数小时。要检查这是否已完成，请在 补丁评估 - 事件查看器 中查看 补丁更新文件 栏。

我们建议您按照以下说明采用补丁策略。

1. 使用“保护计算机向导”部署补丁代理到计算机中。（在向导的 选择功能 页面中，选择 补丁。）

   注释
   如果“保护计算机向导”已经在运行 Enterprise Console ，但尚未安装补丁代理，则必须运行“保护计算机向导”重启对计算机的保护。

2. 启用您的默认的补丁策略中的补丁评估。
   在这之后，您将具有针对整个网络的一个补丁策略。
3. 使用“补丁评估事件查看器”，查看哪些计算机漏掉了补丁，哪些计算机已及时更新。单击 查看 > 补丁评估事件，您可以访问“事件查看器”。

   注释
   您必须以手动方式在计算机上安装漏掉的补丁。

4. 如果您要求针对不同的组，能够启用或禁用补丁策略，或者，指定不同的补丁评估频率，那么，请为不同的组创建不同的策略。

要了解更多有关设置补丁策略的信息，请参见 Sophos Enterprise Console帮助。

11 设置网页控制策略

11.1 建议的设置

配置网页控制，有两种策略可以选择：不合适的网站控制和完全网页控制。根据您将要选择的策略，建议的设置会有所不同。在设置您的网页控制策略时，请考虑：

不合适的网站控制

- 查看针对各个网站类别的措施，并调整这些措施以适应您的公司或计算机组。要使不同的计算机组能够访问的网页不同，请为不同的组创建不同的策略。例如，可能有些网站，比如 Facebook，您只想人事部门能够访问。
- 在展开部署策略之前，规划一份网站免除列表。通过 网站例外 标签，您可以手动输入您想要从策略中排除的网站。例如，您可能有一些无需过滤的本地网址，或者，您想要在已允许的网站类别中阻断某些网站。
- 使用网页控制“事件查看器”可以快速筛选要仔细查看的事件。单击 查看 > 网页事件，您可以访问“事件查看器”。基于所显示的措施，您可以调整网站类别的设置。

完全网页控制

重要提示
您必须有 Sophos Web Appliance 或 Security Management Appliance，以便使用完全网页控制。

- Sophos Web Appliance 配置指南和 Security Management Appliance 配置指南中有设置您的网页设备的总体指导说明。网页设备提供了安装向导帮助您选择最适合您的设置。
- 您可能会为不同类型的用户配置不同的策略。请参见 Web Appliance 的在线产品技术文档了解详情。

  Sophos Web Appliance 文档可以在 http://wsa.sophos.com/docs/wsa/ 中找到。
- 在展开部署策略之前，请规划网页控制策略的例外情况。例如，您可以使用“特殊时间”功能，使得在正常的工作时间之外（如：午休时间）可以访问某些网站。您还可以为特定的用户创建“附加的策略”，这些策略例外于“默认策略”和“特殊时间策略”。
- 您需要考虑，如果无法确定某个网站的类别时，您想要 Sophos Web Appliance 采取什么措施。勾选框 如果无法确定网站的分类，则阻断浏览。 不是默认选项。这意味着，如果无法对某网站分类时，将会允许继续浏览该网站。在选择了此勾选框之后，当此服务恢复时，无法分类的那些 URL 将会被阻断。

要了解更多信息，请参见 Sophos Enterprise Console 和 Sophos Web Appliance 技术文档。

11.2 怎样展开部署网页控制策略

首先，决定使用哪种网页过滤模式：不合适的网站控制或完全网页控制。您必须有 Sophos Web Appliance 或 Security Management Appliance，以便部署完全网页控制。

要了解更多有关设置网页控制策略的信息，请参见 Sophos Enterprise Console帮助。

11.2.1 怎样展开部署不合适的网站控制策略

此基本网页控制选项包括 14 种基本的网站分类。它用于防止用户访问不合适的网站。在应用实施某个网页控制策略时，请考虑：请参见 Enterprise Console 文档，获取具体的指导说明。

1. 请确保网页控制策略已启用。
2. 如果您的公司有合理使用因特网的制度，那么，您应该相应地调整您的设置，避免用户访问到可能被视为违法制度的不合适的网站。
3. 要使不同的计算机组能够访问的网站不同，请为不同的组创建不同的策略。
4. 考虑哪些计算机组需要网页控制，以及适合各个计算机组的策略类型。
5. 查看针对各个网站类别的默认措施。如果您想要应用不同的措施，请从下拉列表中选择它。考虑您想要阻断用户访问哪些网站类别，可以访问哪些网站类别，以及当用户访问哪些网站类别时，需要发出警告。
6. 确定哪些网站可以免除过滤机制的检查，并将这些网站添加到 要允许的网站 列表或 要阻断的网站 列表中。

   注释
   如果在“阻断”和“允许”列表之间有冲突或重复的条目，那么，在“阻断”列表中的条目具有优先权。例如，如果在“阻断”列表和“允许”列表都包含一个相同的 IP 地址，那么，该网站将会被阻断。另外，如果某个域名包含在“阻断”列表中，但是它的子域名包含在“允许”列表中，那么，“允许”列表中的条目会被忽略，该域名及其所有子域名都将被阻断。

7. 使用“网页控制事件查看器”查看过滤的结果。单击 查看 > 网页事件，您可以访问“事件查看器”。使用“事件查看器”查看网页事件。您可以根据查看的结果，调整策略。

要了解更多信息，请参见 Enterprise Console 技术文档：

11.2.2 怎样展开部署完全网页控制策略

此模式使用完全网页策略。它可以强制实施综合的，全功能的网页控制策略，并提供有关网页通讯流的完整报告。此选项要求 Sophos Web Appliance 或 Security Management Appliance。

1. 按照网页设备文档中的说明，配置您的 Sophos Web Appliance 或 Security Management Appliance，确保已开启了 终结点网页控制。
2. 确保网页控制在 Enterprise Console 上已启用。
3. 如果您的公司有合理使用因特网的制度，那么，您应该相应地调整您的设置，避免用户访问到可能被视为违法制度的不合适的网站。
4. 要使不同的用户组能够访问网站有所不同，请为各个用户组创建不同的策略。
5. 确定您想要控制的网站。您想要用户避免访问哪些网站类别？哪些可以访问的网站类别？您想要用户在访问哪些网站类别时，受到警告信息？
6. 确定您想要视为例外的网站，并将它们添加到网页设备的“本地网站列表”中。
7. 在“完全网页控制”模式中，您可以使用 Sophos LiveConnect 选项。您可以配置网页设备使用 LiveConnect，以便策略的更新文件能够部署给用户，以及上传来自用户的计算机的报告数据，（即使当用户没有连接在网络中时。）

要了解更多信息，请参见 Sophos Enterprise Console 和 Sophos Web Appliance 技术文档。

12 设置漏洞防御策略

12.1 建议的设置

漏洞防御策略指定安全软件如何防御勒索软件和其他形式的恶意软件攻击。

注释
默认情况下，所有漏洞防御选项都是开启的。

建议您使用默认设置。

12.2 怎样展开部署漏洞防御策略

默认情况下，易受攻击的应用程序将受到保护。在漏洞防御中排除应用程序时需要非常小心。它们仍然受到 CryptoGuard 和安全浏览保护。

我们建议您按照以下说明展开部署漏洞防御策略：

1. 所有漏洞防御选项在默认情况下都是开启的。建议您使用默认设置。在修改设置前，您应该监视所有漏洞防御事件一段时间。
2. 使用漏洞防御事件查看器监视漏洞防御事件。您可以通过单击事件 > 漏洞防御事件，访问事件查看器。
3. 根据您的监视情况修改漏洞防御策略。例如，您可能想在攻击缓解中排除一些应用程序或攻击事件。有关详细信息，请参阅 Sophos Enterprise Console帮助，配置策略 > 漏洞防御策略部分。

   重要提示
   为提高安全性，我们建议您基于攻击事件的指纹进行排除，而不是排除整个应用程序。

   a) 创建新策略或修改默认策略。
   b) 检查策略中是否有任何弱项。
   c) 在需要有所不同时，请在组中划分出子组，并创建额外的策略。
4. 按要求分配您的策略。

有关设置漏洞防御策略的详细信息，请参阅 Sophos Enterprise Console帮助。

13 扫描建议

以下部分中的扫描选项都是设置在“防病毒和 HIPS 策略”中的。在设置扫描选项时，请考虑：

- 尽可能使用默认设置。
- 尽可能地在 Enterprise Console 中，而不是在本地计算机上设置扫描。
- 考虑计算机的角色（例如：台式机或服务器）。

扩展名

要找到读写扫描中的扩展名选项，请在 防病毒和 HIPS 策略 对话框中，单击 启用读写扫描 旁的 配置，然后，转到 扩展名 标签页。

对于计划扫描，请在 防病毒和 HIPS 策略 对话框中的 计划扫描 下，单击 扩展名和排除项目。

- 扫描所有文件 选项通常不需要，也不建议使用。通常，选择 只扫描可执行文件和其它薄弱文件 选项，扫描由 SophosLabs 发现的各种安全隐患。只在技术支持人员的建议下使用“扫描所有文件”。

其它扫描选项

要找到读写扫描中的其它扫描选项，请在 防病毒和 HIPS 策略 对话框中，单击 启用读写扫描 旁的配置。

对于计划扫描，请在 防病毒和 HIPS 策略 对话框中的 计划扫描 下，选择扫描，并单击 编辑。在计划扫描设置 对话框，单击 配置。

- 扫描打包文件内部 选项，会使扫描的时间增加，并且通常没有必要进行。当您试图访问打包文件中的内容时，该文件会被自动扫描。因此，我们也不建议选择此选项，除非您需要频繁使用打包文件。
- 我们建议扫描计算机系统内存，防范安全隐患。计算机的操作系统使用系统内存。您可以在启用读写扫描的情况下，定时在后台扫描系统内存。您还可以在计划扫描中包括系统内存扫描。依照默认值，扫描系统内存 选项是启用的。

14 使用读写扫描

在使用读写扫描时，请考虑：

- 尽可能使用默认设置。
- 在 读文件时，写文件时，以及 重命名文件时 扫描的选项，依照默认值是启用的，这针对新安装的软件。对于升级的软件，您必须另行启用它们。
- 如果安装了某些加密软件，那么，读写扫描可能会检测不到病毒。更改启动进程，确保在读写扫描开始时，加密的文件已被解密。要了解更多有关怎样针对加密软件使用防病毒和 HIPS 策略的信息，请参见 Sophos 技术支持知识库文章 12790 (http://www.sophos.com/en-us/support/knowledgebase/12790.aspx)。
- 当您没有选择读写扫描时，请确保计算机使用计划扫描。要了解更多信息，请参见使用计划扫描（第 27 页）。

警告
请意识到禁用读写扫描会增加计算机的安全风险。

15 使用计划扫描

在使用计划扫描时，请考虑：

- 尽可能使用默认设置。
- 使用计划扫描，作为评估安全隐患或估计不需要的程序或受控程序的普遍性。
- 当您没有选择读写扫描时，请确保计算机使用计划扫描。将这些计算机放置到某个组中，并定义某个计划扫描。
- 请意识到进行计划的扫描时，对计算机的运行效率可能造成的影响。例如，如果您要计划扫描某个频繁读写数据库的服务器，请考虑在对它的运行效率造成的影响最小时，进行扫描。
- 对于服务器，请考虑它所负担的工作任务。如果是进行备份工作的服务器，那么，不要在进行备份工作的同一时间，安排进行计划扫描。
- 在设定的时间扫描。请确保在各台计算机上，每天定时（如：上午 9 点）执行一次计划扫描。计划的扫描应该至少每周在所有的计算机上运行一次。
- 以较低的优先级运行扫描 选项允许在 Windows Vista 及以后的操作系统中运行的计划扫描以较低的优先级运行扫描，以便最大限度地降低对用户的应用程序的影响。建议使用此选项；不过，选用了此选项的扫描会花费更长的时间来完成扫描。

16 使用即时扫描

在使用即时扫描时，请考虑：

- 在要求手动评估或清除时，使用即时扫描。

17 从扫描中排除项目

按照以下说明从扫描中排除项目：

- 使用扩展名从扫描中排除特定的文件类型。
- 使用扩展名从扫描排除特定的项目，如：文件或驱动器。您可以创建驱动器级的排除项目 (X:)，目录级的排除项目 (X:\Program Files\Exchsrvr\)，或者，文件级的排除项目 (X:\Program Files\SomeApp\SomeApp.exe)。
- 考虑为不断需要使用介质驱动器的特定用户，从扫描中排除介质驱动器。介质驱动器读取和写入临时文件，当每次使用它时，各文件都会被扫描，这会增加扫描的时间。
- 如果您不想扫描远程文件（在网络资源中），请使用 排除远程文件 选项。我们建议所有计算机在访问远程文件时，都对它们进行扫描；不过，您可能会在文件服务器上，或者，在远程访问大量或不断更改的文件的特定情况下，选择此选项。

警告
请意识到从扫描中排除项目会增加计算机的安全风险。

18 技术支持

您可以通过以下各种方式获得 Sophos 产品的技术支持：

- 访问 community.sophos.com/ 的 Sophos Community 论坛，并搜索遇到相同问题的其它用户。
- 访问 www.sophos.com/zh-cn/support.aspx 的 Sophos 技术支持知识库。
- 在 www.sophos.com/zh-cn/support/documentation.aspx 中下载产品的技术文档。
- 访问 https://secure2.sophos.com/support/contact-support/support-query.aspx 联系我们的技术支持团队。

19 法律声明