Symantec™ Email Security.cloud

服务说明

2018 年 9 月

本《服务说明》描述了 Symantec Email Security.cloud 服务（以下称“本服务”）。本说明中所有加粗术语的含义如“协议”（定义见下文）或“定义”部分中所述。

本《服务说明》连同通过引用包括在内的任何附件，构成客户与 Symantec（赛门铁克）之间手动或电子签署的用于规范本服务使用的协议的一部分，如果不存在此类签署的协议，则构成“Symantec（赛门铁克）联机服务条款与条件”（以下称“协议”）的一部分。

目录

1: 技术/商业功能和性能

- **服**务概述
- **服**务选项和功能
- **服**务级别协议
- **支持的平台和技**术要求
- **托管服**务软件组件

2: 客户责任

- **可接受的使用策略**

3: 权利和订购信息

- **收**费标准
- 订购变更

4: 协助与技术支持

- **客**户协助
- **技**术支持
- 对服务和**/或支持服**务基础架构的维护

5: 附加条款

6: 定义

附件 A 服务级别协议

Symantec™ Email Security.cloud

服务说明

2018 年 9 月

1: 技术/商业功能和性能

服务概述

Symantec™ Email Security.cloud 是一款托管服务，可过滤电子邮件，帮助企业抵御恶意软件（包括目标性攻击和网络钓鱼）、垃圾邮件和不需要的群发邮件。该服务可提供加密和数据保护选项，帮助企业控制电子邮件发送的敏感信息。服务支持多个供应商的多种邮箱类型。

服务功能

- 客户管理员可使用安全密码保护登录访问服务管理控制台。客户可以在管理控制台中配置和管理服务、访问报告，查看本服务提供的数据和统计信息。
- 本服务将 24x7 全天候运行，随时可通过服务了解硬件可用性、服务容量和网络资源利用率。定期监控本服务还可了解服务级别的遵从状况，并按需进行调整。
- 本服务的报告功能可通过管理控制台访问。报告内容包括活动日志和/或统计信息。客户可采用管理控制台选择生成报告，该报告可配置为定期通过电子邮件发送，或从管理控制台下载。
- 本服务旨在让客户实施有效且强制性的计算机使用策略或类似规则。
- 由 Symantec（赛门铁克）提供的建议字词列表及模板规则或策略可能包含某些被视为失礼的字词。
- 如因任何原因导致服务暂停或终止，Symantec（赛门铁克）可以撤消在置备本服务时所做的全部配置更改。恢复服务后，由客户负责执行所有其他必要的配置更改。

服务选项和功能

服务有两种选项：Email Protect 或 Email Safeguard。选定选项或加载项的每位用户必须购买本服务（遵守本《服务说明》中的限制）。

各服务选项的功能

	Email Protect	Email Safeguard
Email Antimalware：恶意软件防护，包括网络钓鱼防护和目标性攻击防护	✓	✓
Email Antispam：垃圾邮件和网络钓鱼（实时链接跟踪），以及群发邮件防护	✓	✓
Email Data Protection：可自定义的内容过滤策略控制		✓
Email Image Control：不良图像检测		✓
出站过滤	✓	✓
强制性 TLS 加密		✓
随机性 TLS 加密	✓	✓
地址注册：无效收件人处理	✓	✓
用户和组 LDAP 同步工具	✓	✓

消息跟踪	✓	✓
报告控制板	✓	✓
汇总报告 (PDF) 和详细报告 (CSV)	✓	✓
最终用户垃圾邮件隔离门户和通知	✓	✓
免责声明管理	✓	✓
Policy Based Encryption Essentials		✓
电子邮件仿冒控制		✓

有关具体服务功能的其他信息，请参阅联机帮助：http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ZH_CN。

服务加载项

	Email Protect	Email Safeguard
Advanced Threat Protection: Email	可用	可用
Policy Based Encryption Advanced	_	可用
Email Fraud Protection	可用	可用
Email Threat Isolation	可用	可用

有关具体服务加载项的其他信息，请参阅联机帮助：http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ZH_CN。Email Fraud Protection 的《服务说明》位于：https://www.symantec.com/about/legal/repository.

Advanced Threat Protection: Email 利用 Symantec Cynic™ 沙盒检测以电子邮件形式发送的高级威胁，识别向目标企业或用户发起的目标性电子邮件攻击，并运用 Symantec Click-time™ URL Protection 识别在发送电子邮件后变为恶意网站的 URL。能够在发送电子邮件后为 O365 客户撤回 Cynic™ 沙盒确定的恶意电子邮件。它可提供详细的恶意软件报告，包括 URL 信息、恶意软件类别、检测方法和文件哈希。增加 Data Feed API 以通过经验证的 URL 提取恶意软件报告数据，无需导入文件或通过电子邮件传送数据。Advanced Threat Protection: Email 还提供对 Phishing Readiness 服务的访问权限，该服务是一个网络钓鱼攻击模拟器，用于确定人员对此类攻击的易感性。Phishing Readiness 服务的使用受条款和条件的约束 (https://www.symantec.com/about/legal/repository)。

Policy Based Encryption Advanced 可提供：(i) 提取式 Web 访问门户；(ii) PGP 和 S/MIME 传递支持；(iii) 在尝试 TLS 加密无效之后，再用较不透明的加密技术；(iv) 推送加密的 .pdf 文件（Email Safeguard 计划中 Policy Based Encryption Essentials 功能所包含的唯一加密方法）。Policy Based Encryption Advanced 按发送用户进行授权许可，用户量可能是 Email Safeguard 选项的整体用户数的一部分。如果客户要求使用 Policy Based Encryption Advanced 选项进行安全声明传递，Symantec（赛门铁克）会让客户依据 Symantec（赛门铁克）指定的公式，按照要传递的声明数量购买额外的用户许可证。

Symantec™ Email Fraud Protection 是一款云服务，该服务会自动强制执行 DMARC（基于域的消息身份验证、报告和一致性）。与手动方法相比，Symantec Email Fraud Protection 使得 DMARC 强制执行的每一步更简单，更无缝。强制执行可降低入站仿冒攻击的风险，因为来自未经身份验证的来源的所有电子邮件都会被隔离或拒绝。一旦强制执行，电子邮件收件人或邮件传输代理知道他们可以信任客户域，从而提高电子邮件的可传送率。

Symantec™ Email Threat Isolation 通过隔离恶意链接并安全呈现风险网页来加强对鱼叉式网络钓鱼、凭据盗用和高级电子邮件攻击的防护。Email Threat Isolation 使 Symantec（赛门铁克）能够针对利用恶意链接的复杂电子邮件威胁（例如，高级鱼叉式网络钓鱼或凭据盗用攻击）提供最强大的保护。

Email Threat Isolation 在用户及其电子邮件链接之间创建安全的执行环境，远程呈现可疑链接并仅向用户显示安全的 Web 内容。因此，Symantec（赛门铁克）会阻止任何包含恶意链接的威胁到达用户，因为它收到的每条链接都会被视为恶意链接并以远程方式执行，从而使用户及其设备免遭威胁攻击。Email Threat Isolation 还通过以只读模式呈现网络钓鱼网站来阻止凭据式网络钓鱼攻击，从而防止用户输入公司凭据和其他敏感信息。

服务级别协议

- Symantec（赛门铁克）将为本服务提供适用的服务级别协议（以下称“SLA”），如附件 A 所指定。

支持的平台和技术要求

- 有关本服务支持的平台和技术要求，请参见 http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ZH_CN。

托管服务软件组件

- 本服务包括管理控制台中提供的软件服务组件，支付相应费用后即可访问。

2: 客户责任

Symantec（赛门铁克）只能在客户提供了必要信息或执行了必要操作的情况下执行本服务，否则 Symantec（赛门铁克）对本服务的执行可能会被推迟、影响或阻止，而且/或者客户享受《服务级别协议》的优惠机制可能会归于无效，详见下文。

- 设置信息支持：客户必须提供所需要的信息，以便 Symantec（赛门铁克）开始提供本服务。
- 充足的客户人手：应 Symantec（赛门铁克）合理请求，客户必须提供充足的人手来协助 Symantec（赛门铁克）交付本服务。
- 客户负责保管其帐户信息、密码或其他登录凭据。
- 客户同意使用合理方式保护该凭据，并就对客户帐户的任何已知的未经授权的使用告知 Symantec（赛门铁克）。
- 续订凭据：如果适用，客户必须应用帐户管理中适用的订购授权书或订单确认书提供的续订凭据来继续享受本服务，或者在本服务的有效期内继续保留可用的帐户信息和客户数据。
- 客户配置与默认设置：客户必须通过管理控制台配置本服务的功能（如适用），否则将应用默认设置。某些情况下不存在默认设置，此时，客户必须选择一项设置，否则无法提供本服务。本服务的配置与使用完全由客户掌控，因此，对于客户对本服务的使用以及因使用本服务而可能产生的任何民事或刑事责任，Symantec（赛门铁克）概不承担任何责任。

可接受的使用策略

- 客户负责遵守《Symantec（赛门铁克）联机服务可接受的使用策略》。

3: 权利和订购信息

收费标准

本服务按照订单确认书中指定的以下标准提供：

- “**用户**”是指经授权可以使用本服务和/或从使用本服务中受益，或实际使用本服务中任何部分的个人和/或设备。

订购变更

如果客户已直接从 Symantec（赛门铁克）收到客户订购或权利，则有关客户订购或权利的许可变更的相关通知必须发送到以下地址（或 Symantec（赛门铁克）公布的备用地址）：CLD_cancellations_MLABS@symantec.com，除非客户与 Symantec（赛门铁克）签署的协议中另

有规定。根据此流程发送的任何通知以实际收到之日为准。如果客户通过 Symantec（赛门铁克）经销商收到客户订购或权利，请联系客户经销商。

4: 协助与技术支持

注意：只有客户有权直接从 Symantec（赛门铁克）接受客户协助与支持（以下称“支持”），本节才适用。如果客户有权从 Symantec（赛门铁克）经销商获得协助与支持，请参见客户与经销商之间的协议以了解有关此类支持的详细信息，且此处所述的支持将不适用于客户。

客户协助

作为本服务的一部分，Symantec（赛门铁克）将在当地工作时间内提供以下协助：

- 接收和处理有关本服务实施方面的订单；
- 接收和处理对本服务各类功能进行修改的许可请求，以及
- 回答有关账单和开票的问题。

技术支持

入门级支持作为以下指定的服务的一部分随附。

- 提供 24x7 全天候支持，协助客户对本服务各类功能进行配置并解决所报告的与本服务相关的问题。服务支持将根据以下网页上发布的条款和条件以及技术支持策略执行：https://support.symantec.com/en_US/article.TECH236428.html。
- 一旦向客户提交的支持案例分配严重性级别，Symantec（赛门铁克）就将尽一切合理努力按照下表中定义的响应目标做出响应。因客户的操作而产生的故障或需要其他服务提供商采取操作的故障均在 Symantec（赛门铁克）控制范围以外，因此本支持承诺不适用。

问题严重性	**24X7 全天候支持响应目标***
一级严重性：发生的问题没有立即可用的应急措施，具体情形包括：(i) 客户的生产服务器或其他任务关键系统停机了，或是服务实质上已丧失；或 (ii) 客户的任务关键数据面临丢失或损坏的严重风险。	30 分钟内
二级严重性：发生的问题导致主要功能受到严重影响。虽然客户可以采用受限的方式继续执行操作，但从长远角度看，生产效率会受到不利影响。	最多 2 小时
三级严重性：发生的问题对客户的业务运营产生有限的负面影响。	下个工作日的同一时间之前**
四级严重性：发生的问题未对客户的业务运营造成不利影响。	下个工作日内；另外，Symantec（赛门铁克）还建议客户在 Symantec（赛门铁克）的论坛上提交对新功能或改进的建议

以上支持响应目标可在正常服务运营期间实现，但在对以下“维护”小节中所述的服务和/或支持基础架构的维护期间不适用。

**目标响应时间与请求响应时间相关，不与解决时间（解决请求所花费的时间）相关。*

***“工作日”是指客户当地时区的标准区域工作时间和工作日，不包括周末和当地节假日。大多数情况下，“工作时间”是指客户当地时区的上午 9:00 到下午 5:00。*

对服务和/或支持服务基础架构的维护

Symantec（赛门铁克）会不定期进行维护。Symantec（赛门铁克）将尽商业上合理的努力选择非客户集中使用时间进行例行维护操作，最大限度降低服务中断。此等例行维护活动将不提前通知客户。对于以下列出的所有其他类型的维护，Symantec（赛门铁克）将竭尽全力提前通知受影响方，通知方式是在 Symantec（赛门铁克）状态页面 (https://status.symantec.com/) 上发布相关警报。有关服务状态、计划维护和已知问题的信息，请访问 Symantec（赛门铁克）状态页面并订阅 Symantec Email Security.cloud 页面，以接收最新更新。**安全性扫描和电子邮件传送等核心服务功能在所有维护活动期间不会被中断。**

- ***计划维护：*** 计划维护是指计划内维护周期，期间可能因服务基础架构不可用而导致服务中断或暂停。在进行计划维护时，Symantec（赛门铁克）将竭尽全力选择受影响基础架构所在时区内的非客户集中使用时间进行维护操作，且维护仅限于部分网络，而非全部网络。在计划维护期间，本服务可能被转向基础架构中未进行维护的部分，以避免服务中断的可能。对于计划维护，Symantec（赛门铁克）将尽商业上合理的努力，通过在 Symantec（赛门铁克）状态页面发布通知的形式提前七 (7) 天通知客户。客户也可以在订阅 Symantec（赛门铁克）状态页面后通过短信、电子邮件或 Twitter 接收通知。
- ***非计划维护：*** 非计划维护是指无法按标准提前七 (7) 天发出通知的计划内维护周期，其间可能因服务基础架构不可用而导致服务中断或暂停。Symantec（赛门铁克）将尽商业上合理的努力，通过在 Symantec（赛门铁克）状态页面发布通知的形式至少提前一 (1) 天通知客户。在非计划维护期间，本服务可能被转向基础架构中未进行维护的部分，以避免服务中断的可能。有时，Symantec（赛门铁克）将进行紧急维护。紧急维护是指*必须在可能的情况下尽快进行的维护以解决或预防重大事件*。Symantec（赛门铁克）将竭尽全力提前通知受影响方，通知方式是在维护开始前至少一 (1) 个小时在 Symantec（赛门铁克）状态页面上发布相关警报。
- ***管理控制台维护：*** 对于管理控制台维护，Symantec（赛门铁克）将尽商业上合理的努力，通过在 Symantec（赛门铁克）状态页面发布通知的形式提前十四 (14) 天通知客户。Symantec（赛门铁克）将竭尽全力选择非客户集中使用时间进行管理控制台的维护，以尽量降低对管理控制台可用性的影响。有时，Symantec（赛门铁克）可能会对管理控制台进行细微更新，此等例行维护活动将不提前通知客户。

5: 附加条款

- 本服务可以在全球范围内进行访问和使用，但应根据当时最新的 Symantec（赛门铁克）标准，遵循适用的出口法规限制和技术限制。
- Symantec（赛门铁克）有权出于提供同等或强化服务的目的（只要 Symantec（赛门铁克）不会严重降低本服务的核心功能），修改并更新本服务的特性和功能。客户承认并同意，Symantec（赛门铁克）有权在订购期内的任何时候更新本《服务说明》，以正确反映当前提供的服务，且更新的《服务说明》自发布之时起生效。
- 使用任何软件形式的服务组件都应遵守此软件随附的授权许可协议。如果服务组件没有对应的 EULA，则应遵守下列地址中规定的条款和条件：http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf。与使用此类服务组件相关的任何其他权利和义务都应在《服务说明》中进行规定。
- 除非《服务说明》中特别指定，否则，本服务（包括任何随附托管服务软件组件）可使用开源代码及其他第三方材料，但需要另外获得许可证。
- Symantec（赛门铁克）可随时更新本服务，以保持服务的有效性。
- 由 Symantec（赛门铁克）提供的任何模板仅作为指南用于帮助客户创建自己的自定义策略及其他模板。
- 本服务具有以下限制：
    - 入站和出站邮件，每位用户每个月的上限为一万 (10,000) 封。该限制并不适用于客户收到的垃圾邮件和恶意软件。
    - Symantec（赛门铁克）有权在客户使用量超出邮件限制时，在通知客户的情况下向客户开票收取新增用户在服务合同剩余月份里的费用。
    - 入站和出站邮件重试调度为七 (7) 天。
    - 默认的最大电子邮件大小为 50 MB。客户可任意指定电子邮件大小上限，最高不得超过 1000 MB。服务接收的任何电子邮件若超过指定限制即会予以拦截及删除，并向发件人、指定收件人和管理员发送通知提醒电子邮件。
    - “消息跟踪”是指可搜索 30 日内的数据进行故障排除，一次搜索返回的结果数另有限制。
    - “恶意软件隔离”是指电子邮件会在三十 (30) 日后自动删除。
    - “垃圾邮件隔离”是指电子邮件会在十四 (14) 日后自动删除，除非配置为其他数值。

  - 控制板报告数据可用性 = 详细信息的可用性为四十 (40) 天；汇总信息的可用性为十二 (12) 个月。
  - 汇总报告 (PDF) 数据可用性为十二 (12) 个月。
  - 详细报告 (CSV) 数据可用性为四十 (40) 天。

- Policy Based Encryption 具有以下限制：
  - Policy Based Encryption (Z) 每位用户每个月的出站邮件上限为三百 (300) 封。
  - Policy Based Encryption Essentials/Advanced 每位用户每个月的出站电子邮件上限为四百八十 (480) 封。
  - 发送至多个收件人时，每个不重复地址会算作一个安全电子邮件。如果客户单月超出了允许的安全电子邮件数量，Symantec（赛门铁克）有权向客户开票收取实际使用量的费用。
  - 通过 Policy Based Encryption 服务路由的电子邮件最大不得超过 50 MB。
  - 如果使用 Policy Based Encryption (Z) 服务的提取式加密，默认情况下，电子邮件会在安全提取门户中存储 90 天后过期。
  - 如果使用 Policy Based Encryption Advanced 服务的提取式加密，默认情况下，电子邮件会在安全提取门户中存储 30 天后过期。
  - 可用性和延迟服务级别并不适用于本服务。

- 为确保邮件在传输过程中安全无虞，Symantec（赛门铁克）建议客户将用于 Policy Based Encryption 的域配置为在服务基础架构的所有出站和入站电子邮件中强制实施 TLS 加密。
- 客户必须采用 Symantec（赛门铁克）提供的路由信息，通过 Symantec（赛门铁克）路由其入站电子邮件，而不得将电子邮件路由至特定的机房或 IP 地址。
- 本服务仅面向拥有自己电子邮件域名且可以配置该域名的 MX 记录和/或 DNS 的客户。
- 客户必须接收来自所有必需 IP 范围的入站电子邮件，确保在部分服务基础架构不可用时服务仍可以连续运行。
- 客户必须指定入站电子邮件传递到企业的邮件服务器 IP 地址或主机名。
- 客户必须确保需要使用服务的所有域（包括子域）已经置备完毕。客户同意，对于未置备的域，服务功能可能无法正常运行，电子邮件可能无法送达。客户同意提供并维护接收服务的有效电子邮件地址列表（以下简称“验证列表”）。客户负责在服务开始前以及在整个服务期间确认验证列表。对于发送到验证列表以外的地址或拼错的地址的电子邮件，所有邮件都会遭到服务拒绝。客户同意 SLA 不适用于发送至无效地址的电子邮件。为免产生疑问，使用垃圾邮件隔离功能的客户必须维护验证列表，并且启用地址注册功能。如果客户无法提供此类验证列表，而且请求禁用地址注册功能，Symantec（赛门铁克）将根据具体情况审查每个此类请求，并保留全权决定拒绝请求的权利。
- 客户可能会发出包含恶意软件或垃圾邮件类的电子邮件，或请求 Symantec（赛门铁克）在客户域中分发此类邮件。 客户同意，对于应客户请求分发此类电子邮件造成的任何后果，Symantec（赛门铁克）概不承担任何责任。
- 对于因服务未能识别垃圾邮件或错将电子邮件视为恶意软件或垃圾邮件而造成的任何直接或间接损坏或损失，Symantec（赛门铁克）概不承担任何责任。Symantec（赛门铁克）有权扫描所有出站电子邮件。
- 从服务部署之时起，经本服务扫描的所有电子邮件都会应用默认的免责声明消息，客户可通过管理控制台编辑该消息文本。Symantec（赛门铁克）保留随时更新默认免责声明消息的权利。
- 客户应遵守与使用本服务有关的所有适用法律。在某些国家/地区，可能需要征得个人同意。本服务的配置与使用完全由客户掌控，因此，对于客户的服务使用情况以及因使用本服务而可能产生的任何民事或刑事责任，Symantec（赛门铁克）概不承担任何责任。
- 如果出于安全原因无法继续向客户提供本服务，包括（但不限于）黑客攻击、拒绝服务攻击、邮件炸弹或其他针对或来自客户域的恶意活动，客户同意 Symantec（赛门铁克）可以暂时停止向客户提供本服务。如遇上述情形，Symantec（赛门铁克）会立即通知客户并与客户合作解决此类问题。一旦解除安全威胁，Symantec（赛门铁克）将立即恢复本服务。
- 如果服务出于任何原因暂停，服务不会应用到客户的电子邮件，而且电子邮件不会通过 Symantec（赛门铁克）的基础架构路由。在服务暂停期间，客户必须负责重新定向其电子邮件，并且确认所有配置在服务恢复时是正确的。
- 若服务因任何原因终止，客户帐户会被删除，且客户将无法访问服务。
- 客户不得允许系统：(i) 充当开放式中继或开放式代理；(ii) 发送垃圾邮件。Symantec（赛门铁克）保留随时审查客户是否遵循本节条款的权利。为避免疑义，凡违反本条款的任何行为即构成重大违反许可协议的情况，Symantec（赛门铁克）有权立即暂停所有或部分服务，直到违反情况予以改正为止，亦或有权终止与受影响服务相关的许可协议。

- 若在任何时候 (i) 客户的电子邮件系统被列入黑名单，或 (ii) 因客户传送垃圾邮件，而造成 Symantec（赛门铁克）系统被列入黑名单，或 (iii) 客户未能履行本《服务说明》中所载的任一义务，Symantec（赛门铁克）将通知客户，并保留自行决定是否立即暂缓部署、暂停或终止所有或部分服务的权利。
- 客户只能将服务用于客户自身的业务目的。客户同意不转售、再授权、出租或以其他方式将服务及相关文件提供给任何第三方使用。客户同意，未经 Symantec（赛门铁克）事先书面同意，不得将服务用于构建竞争产品或服务，不得以公开发表为目的而复制服务功能或用户界面、执行服务评估、效能评析或其他比较分析。

6: 定义

“**地址注册**”为服务的强制功能，自动拒绝目标邮件地址不在客户有效电子邮件地址列表（验证清单）的入站电子邮件。

“**管理员**”是指经授权代表客户管理本服务的客户用户。 根据客户指定，管理员可以管理本服务的全部或部分功能。

“**反垃圾邮件最佳做法设置**”指 Symantec（赛门铁克）建议的服务配置指南，该指南会在客户部署流程中提供给客户，或公布在联机帮助资源中。

“**连接管理器**”是指在 SMTP 握手阶段执行的检测方式。

“**退款申请**”是指客户必须向 Symantec（赛门铁克）提交的电子邮件通知，收件人为 support.cloud@symantec.com，且主题行须注明“退款申请”字样（除非 Symantec（赛门铁克）另行通知）。

“**指定机房群集**”是指指定用于向客户提供 Email Security Services 的两 (2) 个或更多个机房。

“**域级别设置**”是指 Email Security Services 管理控制台中可针对特定域自定义的域设置。

“**电子邮件**”是指由服务传送的任何入站或出站 SMTP 邮件。

“**Email Security Services**”是指 Email Safeguard 及 Email Protect 选项和任何可用的加载项服务。

“**电子邮件恶意软件误报**”是指将合法电子邮件误认为包含恶意软件。

“**最终用户授权许可协议 (EULA)**”是指软件（定义如下）随附的条款和条件。

“**全局设置**”是指在管理控制台中应用于服务的所有域和组级别的操作。

“**组级别设置**”是指在管理控制台中，针对服务适用功能对特定组自定义的组设置。

“**基础架构**”是指用于提供本服务的任何 Symantec（赛门铁克）或许可方技术和知识产权。

“**已知恶意软件**”是指如下恶意软件：Symantec（赛门铁克）收到内容之时，其特征至少已公布一 (1) 小时以供 Symantec（赛门铁克）部署防病毒技术所用。

“**恶意软件**”是指任何用于破坏计算机或移动设备运行的软件，或指无适当授权却用于收集敏感信息及/或擅自访问私人计算机系统的软件。

“**恶意软件误报**”是指将合法电子邮件误认为包含恶意软件。

“**成员**”是指利用旧版电子邮件边界加密加载项服务建立加密网络的客户及其所合作的第三方。

“**月费**”是指本协议中定义的受影响服务的月度费用。

“**联机帮助**”是指以下网址提供的其他信息：http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ZH_CN。

“**开放式代理**”是指配置为允许不明或未经授权的第三方访问、存储或转发 DNS、网页或其他数据供服务使用的代理服务器。

“**开放式中继**”是指配置为接收来自不明或未经授权之第三方的电子邮件，并将电子邮件转发至一位或多位收件人（而这些收件人并非是该电子邮件服务器所连接电子邮件系统的用户）的电子邮件服务器。开放式中继也称为“垃圾邮件中继”或“公开中继”。

“**订单确认书**”是指 Symantec（赛门铁克）联机服务条款与条件（如适用）中所述的含义。如果这些条款和条件不适用于本服务，则“订单确认书”应指本文定义的订购授权书。

“**服务**”是指客户所购 Symantec Email Security.cloud 中的 Email Protect 或 Email Safeguard 选项。

“**服务组件**”指的是作为服务附带部分，Symantec（赛门铁克）可能分开提供的某些支持软件、硬件外围设备以及相关文档。

“**服务退款**”是指在客户提交退款申请且经 Symantec（赛门铁克）验证应向客户退款后，将记入客户下一个发票的金额。

“**服务软件**”是指服务可能需要的软件（定义如下），每个客户计算机必须安装，方可获得本服务。服务软件包括可能由 Symantec（赛门铁克）另行提供的软件及其相关文档，它们也是本服务的一部分。

“**软件**”是指以目标代码形式由 Symantec（赛门铁克）授权给客户的每个 Symantec（赛门铁克）或许可方软件程序，这些程序受随附的 EULA 中的条款和条件约束，包括但不限于此处提供的新版本或更新。

“**垃圾邮件**”是指未经收件人许可的商业电子邮件。

“**垃圾邮件漏报**”是指服务未将垃圾邮件识别为垃圾邮件。

“**垃圾邮件误报**”是指服务将电子邮件误认为垃圾邮件。

“**垃圾邮件建议设置**”是指 Symantec（赛门铁克）建议的服务配置指南，在部署流程中提供给客户或公布在联机帮助资源中。

“**订购授权书**”是指下列一个或多个适用文档，用于进一步定义客户在服务方面的权利与义务：由 Symantec（赛门铁克）发行的 Symantec（赛门铁克）证书或类似文件，或客户与 Symantec（赛门铁克）在服务达成之时、之前或之后签订的书面协议。

“**Symantec（赛门铁克）托管服务条款**”是指位于以下地址或通过以下地址访问的 Symantec（赛门铁克）托管服务条款：https://www.symantec.com/about/legal/service-agreements.jsp。

“**Symantec（赛门铁克）联机服务条款**”是指位于以下地址或通过以下地址访问的联机服务条款和条件：https://www.symantec.com/about/legal/service-agreements.jsp。

“**Symantec 跟踪程序**”是一款用于测算本服务的可用性与延迟时间的 Symantec 工具。

“**机房**”是指一组负载平衡的电子邮件服务器。

“**用户**”是指发送和接收电子邮件并受本服务任何部分保护的个人。

附件 A

服务级别协议

一般条款

- 若 Symantec（赛门铁克）所提供服务未能符合指定的服务级别，客户有权申请服务退款。若客户认为有权要求服务退款，则客户必须于发生疑似未遵守服务级别行为的当月月底的十 (10) 个工作日内提交退款申请。客户应了解相关记录仅会保存有限的天数，因此任何在指定时间范围外提交的退款申请将被视为无效。
- 若要提交退款申请，请联系 Symantec（赛门铁克）技术支持团队。请访问产品支持登录页面，了解详细的指导说明：https://support.symantec.com/en_US/email-security-cloud..html.
- Symantec（赛门铁克）将根据本《服务级别协议》的适用条款对所有退款申请进行验证。Symantec（赛门铁克）可能要求客户提供其他信息以验证退款申请。
- 本《服务级别协议》不适用于下列情况：(i) 计划维护或紧急维护期间，以及因不可抗力及客户或第三方的行为或疏忽导致服务中断期间；(ii) Symantec（赛门铁克）根据此协议条款暂停服务期间；或 (iii) 客户违反此协议（包括但不限于客户有任何逾期发票）；或 (iv) 客户未按照此协议配置服务；或 (v) 服务试用期。
- 本《服务级别协议》规定的补偿应是客户因出现违约、侵权（包括但不限于过失）或其他违反相关服务级别协议而获得的唯一的及排他的补偿。
- 在任何月份，依据本《服务级别协议》，Symantec 给予的最大累计退款金额为：全额月费或一万美元/五千英镑/一万欧元 ($10,000/£5,000/€ 10,000)（依据给客户开具发票的货币），以金额较低者为准。
- 如果受影响的服务作为服务包的一部分进行购买，则将根据受影响的服务而非整个服务包计算服务退款。

Email Security Services 的《服务级别协议》例外情况

本《服务级别协议》不适用于下列情况：(i) 涉及任何未经由本服务传送的电子邮件（包括但不限于客户未执行相应步骤以确保仅接受来自 Symantec（赛门铁克）基础架构的入站电子邮件）；(ii) 或涉及最初发送给 Symantec（赛门铁克）、且每个 SMTP 会话包含超过 500 个收件人的入站或出站电子邮件；(iii) 针对部署于指定机房群集之任一机房的任何客户；或 (iv) 未部署该服务之客户域的任何入站或出站电子邮件。

服务可用性

服务可用性服务级别指的是根据 RFC5321 协议，通过端口 25 从客户 MTA 连接到 Symantec（赛门铁克）基础架构以建立 SMTP 会话的能力。服务可用性服务级别并不适用于管理门户或垃圾邮件隔离系统。服务级别不适用于以下情况：客户未正确配置服务，或因超出 Symantec（赛门铁克）合理控制范围的不可预见情况或原因，包括但不限于自然灾害、战争、恐怖攻击、暴乱、政府行为或 Symantec（赛门铁克）数据中心外的网络或设备故障，包括客户站点的网络故障或客户站点与 Symantec（赛门铁克）数据中心之间的网络故障。

如果在任何月份服务可用性低于百分之百 (100%)，客户可以提交退款申请并按以下百分比获得服务退款，相当于全额月费退款或一万美元/五千英镑/一万欧元 ($10,000/£5,000/€ 10,000) 的退款（依据给客户开具发票的货币），以金额较低者为准：

每月服务可用性百分比	月费退款百分比
99% - 100%	25%
98% - 99%	50%
< 98%	100%

如果在任何月份服务可用性降至百分之九十八 (98%) 以下，在经过 Symantec（赛门铁克）确认后，客户有权终止受影响服务并按照服务终止后的剩余时间，按比例获得预付费用退款。

电子邮件传送

电子邮件传送服务级别指的是 Symantec（赛门铁克）能否完全传送客户入站或出站电子邮件，但需遵守下列条件的限制：

a) Symantec（赛门铁克）必须收到电子邮件；且

b) 电子邮件不得包含恶意软件、垃圾邮件或其他会导致服务拦截的内容。

依据前述条款之规定，如果 Symantec（赛门铁克）无法传递客户的出站或入站电子邮件，且客户未违反本协议条款，客户即有权在三十 (30) 天内，以书面通知方式终止服务。

电子邮件延迟

电子邮件延迟服务级别由以下因素决定：客户指定机房群集内各个机房每隔五 (5) 分钟接收自另一个机房寄出的电子邮件的平均来回时间（由 Symantec（赛门铁克）追踪程序测定）是否超过下表所规定的延迟时间（以月份计算）。若客户认为延迟服务级别未达标准，可提交退款申请，并可能收到根据下表所规定的服务退款：

平均来回时间（秒）	月费退款百分比
60 - 90	25%
90 - 120	50%
120 - 180	75%
> 180	100%

本延迟服务级别不适用于以下情况：

a) 客户未提供 Symantec（赛门铁克）验证清单，且客户遭受拒绝服务攻击；

b) 延迟时间是因往返客户系统的邮件循环传递所造成；

c) 客户的主要电子邮件服务器在初次尝试传递时无法接收电子邮件。

垃圾邮件误报

垃圾邮件误报服务级别规定最高垃圾邮件误报拦截率。垃圾邮件误报服务级别仅适用于以下情况：客户已执行联机帮助资源中所提供的反垃圾邮件最佳做法设置。若任何一个月份的平均垃圾邮件误报拦截率超过客户入站电子邮件流量的 0.0003%，客户可提交退款申请，并可能收到根据下表所规定的服务退款：

垃圾邮件误报拦截率百分比	月费退款百分比
0.0003% - 0.003%	25%
0.003 - 0.03	50%
0.03 - 0.3	75%
> 0.3%	100%

出于本服务级别的目的，下列电子邮件不构成垃圾邮件误报电子邮件：

a) 不属于合法商业电子邮件的电子邮件；

b) 包含 20 位以上收件人的电子邮件；

c) 电子邮件的发件人在客户的阻止发件人列表上，包括但不限于，客户启用用户级别设定时，个别用户定义的阻止发件人列表；
d) 由受感染的计算机发出的电子邮件；
e) 由列在第三方拦截清单上的计算机所发送的电子邮件；
f) 出站垃圾邮件扫描拦截的电子邮件。

客户必须在收到电子邮件的五 (5) 天内，向 Symantec（赛门铁克）技术支持报告疑似误报的电子邮件，才符合服务退款的资格。Symantec（赛门铁克）将会调查并确认电子邮件是否为垃圾邮件误报，并记录调查结果。

垃圾邮件捕获率

垃圾邮件捕获率服务级别是指最低的垃圾邮件拦截率。本服务级别仅适用于以下情况：客户已执行联机帮助资源中所提供的反垃圾邮件最佳做法设置。服务级别对应的是某月份中测得的垃圾邮件漏报数量。客户可提交退款申请，并可能收到根据下表所规定的服务退款：

垃圾邮件拦截率百分比	月费退款百分比
98% - 99%	25%
97 - 98	50%
96 - 97	75%
< 96%	100%

本垃圾邮件拦截率服务级别不适用于以下情况：电子邮件并非传送至有效的电子邮件地址。包含百分之五十 (50%) 以上双字节字符集的电子邮件适用百分之九十五 (95%) 的低垃圾邮件拦截率。一旦此类垃圾邮件捕获率降低到百分之九十五 (95%) 以下，客户则有权要求百分之二十五 (25%) 的服务退款。如果垃圾邮件拦截率低于百分之九十 (90%)，客户有权要求全额月费的服务退款。

客户必须在收到电子邮件的五 (5) 天内，向 Symantec（赛门铁克）技术支持报告疑似漏报的电子邮件，才符合服务退款的资格。Symantec（赛门铁克）将会调查并确认电子邮件是否为垃圾邮件漏报，并记录调查结果。

恶意软件防护

若客户系统因为接收到经过云扫描服务的电子邮件所传送的已知或未知的恶意软件而感染，则客户有权要求如下定义的服务退款金额。客户必须于得知此类恶意软件的五 (5) 天内通知 Symantec（赛门铁克），且此类通知必须经由 Symantec（赛门铁克）记录、调查及验证。客户必须提交退款申请，经过验证属实，客户则会获得服务退款，相当于全额月费退款或一万美元/五千英镑/一万欧元 ($10,000/£5,000/€10,000) 的退款（依据给客户开具发票的货币），以金额较低者为准。本节规定的补偿措施应是客户因出现违约、侵权（包括但不限于过失）或其他因传送到客户的恶意软件或通过服务的第三方造成感染而获得的唯一及排他的补偿。为避免疑义，本节规定的补偿措施不适用于蓄意自我感染。

若通过服务接收的电子邮件中附有恶意软件，且该恶意软件已经自动或透过人为介入在客户系统内启动，客户系统即视为已受感染。若 Symantec（赛门铁克）检测但未拦截带有恶意软件附件的电子邮件，并于 Symantec（赛门铁克）状态页面发布了更新，或已通知客户，并且提供足够信息让客户辨识和删除受感染的电子邮件，则上述补偿措施将不适用。

该服务会尽量扫描所有电子邮件和附件。它无法扫描受发件人直接控制的附件内容（例如，受密码保护和/或加密的附件及/或密码与电子邮件分开发送）。此类电子邮件和/或附件不适用于服务级别，上述规定的补救措施不适用。

本恶意软件防护服务级别不适用于由客户蓄意发布的恶意软件，或在客户的要求下由 Symantec（赛门铁克）蓄意发布的恶意软件。

恶意软件防护服务级别只适用于本《服务说明》中规定的恶意软件，不适用于如下恶意软件：间谍软件、广告软件、指向托管恶意内容的网站的 URL 链接或未知的特洛伊木马。

恶意软件误报

恶意软件误报服务级别指的是最高的恶意软件误报拦截率。若任何一个月份的平均电子邮件恶意软件误报拦截率超过客户电子邮件流量的 0.0001%，客户可提交退款申请，并可能收到根据下表所规定的服务退款：

恶意软件误报拦截率百分比	月费退款百分比
0.0001% - 0.001%	25%
0.001 - 0.01	50%
0.01 - 0.1	75%
> 0.1%	100%

24x7 全天候技术支持和故障响应

Symantec（赛门铁克）24*7 全天候提供技术支持：

a) 为服务发生问题的客户提供技术支持；及

b) 与客户沟通以解决此类问题。