诺顿产品与服务隐私通知 - *最后更新于 2019 年 4 月 29 日*

本通知应与赛门铁克 - 诺顿全球隐私声明一起阅读和应用，并且与该声明相互补充。它描述了诺顿产品与服务收集的数据类别，以及处理这些数据类别的目的。它专门用于向作为数据对象的个人诺顿用户以及向作为数据控制者的中小型企业诺顿用户提供强制透明度信息。请注意，标有星号 (*) 的数据类别是传送给赛门铁克的个人数据，目的是提供相应的诺顿产品特性和服务功能。所有其他数据类别都是由诺顿软件收集，用于以不可识别的形式进行处理。

诺顿的所有产品与服务都遵循赛门铁克 - 诺顿全球隐私声明中规定的高标准。此外，为了向您透明地介绍每种诺顿产品与服务的独有特性和特定目的，除了对产品或服务的描述之外，本通知还描述了我们收集的个人数据以及处理个人数据的目的。

如果您无法接受本通知的任何部分或方面，那么请不要下载、安装或使用相应的产品、服务或其功能，和/或请立即卸载或停止使用任何有关产品、服务或特性。如果产品与服务功能需要您向我们提供额外的个人数据，或者需要您同意处理此类必要的个人数据用于从特定产品或服务的可选功能中获益，那么在下载、安装、激活或使用相关功能时，您将被要求查看本通知，从而能够相应地给出您知情的和具体的同意。

目录

诺顿应用程序锁

产品/服务描述	数据访问和收集	数据处理
诺顿应用程序锁允许用户使用 PIN、密码或图案来保障和保护移动应用程序。如果移动设备丢失或被盗，也可以配置应用程序锁，如果这样配置，那么设备的前置摄像头会在三次尝试解锁设备失败后拍照。	*1. 用户的电子邮箱地址 2. 用户的设置 PIN、移动应用的密码 3. 基于设计的图片，用户可选择	1. 用户的电子邮箱地址会被收集并传送到赛门铁克，以支持诺顿应用程序锁处理密码恢复和重置。 2. 3. 产品从用户输入收集到的所有其他数据都存储在用户的设备上。

诺顿清理

产品/服务描述	数据访问和收集	数据处理
诺顿清理是一种存储最大化工具，它可以扫描用户移动设备的内存缓存来删除广告和不需要的数据，从而释放额外的存储空间。	移动设备的设备唯一标识符 (IMEI)	IMEI 号码从设备中收集并传输给赛门铁克。在传输之后，IMEI 号码在进行任何进一步处理之前被立即散列。进行散列的目的是监视产品的独特用法。一旦数据被散列，就不能追溯到原始设备，因此用户和设备本身都不会受到跟踪或监视。

诺顿错误管理

产品/服务描述	数据访问和收集	数据处理
诺顿错误管理用于记录诺顿产品碰到的问题。在这种情况下，用户可以选择向赛门铁克报告错误。	1. 计算机状态信息（系统语言、国家区域设置、操作系统版本） 2. 进程运行、它们的状态以及性能信息 3. 当诺顿产品遇到问题时，打开的文件和文件夹中的数据	1.-2.-3. 系统信息由赛门铁克处理，目的是纠正遇到的问题，提高诺顿产品的性能。 在某些情况下，如果由于安全威胁或漏洞而遇到错误，赛门铁克可能与更广泛的网络安全社区的合作伙伴（如研究组织和其他安全软件供应商）获取和共享某些非特定用户的或非标识的数据。此类共享的目的在于提高风险意识以及发现和预防风险。赛门铁克也可能使用来自这些信息的统计数据来跟踪和发布关于安全风险趋势的报告。

诺顿社区防卫

产品/服务描述	数据访问和收集	数据处理
诺顿社区防卫使诺顿安全产品用户能帮助提升身份识别，并减少防范新安全威胁的时间。该程序收集选定的安全和应用数据，并向赛门铁克提交数据，以分析新的威胁及其来源。通过分析用户发送的数据，该程序有助于构建更好、更强大的安全产品。 通过加入诺顿社区防卫程序： 1. 通过您和其他参与者提交的数据，您可以参与构建关于网络威胁的更好、更强大的知识，并保护您免受网络威胁。我们的后端技术使用复杂算法来计算在您的机器上下载、安装或运行的每一个文件的安全信誉等级，但是不会做出任何与您或任何其他人个人有关的决定。诺顿安全产品用户获得这种新的创新技术的好处，因为诺顿产品可以： *a. 通过下载智能分析 (Download Insight) 阻止有害下载。诺顿会让您知道您的下载是安全还是不安全，或者它是否有未知的安全配置文件。如果下载不安全，我们的产品会立即采取行动保护您； b. 提供改进的检测率以及减少误报； *c. 通过更快速地清理诺顿社区防卫提交、分析和确定为已知良好的文件，利用诺顿智能扫描 (Norton Insight) 进行更快速的扫描。 2. 通过提供关键的安全和应用程序数据，您可以贡献必要的情报，用于识别新威胁并在它们进一步恶化之前阻止它们。 *诺顿智能扫描仅适用于 Windows 操作系统。	1. 机器 ID（赛门铁克生成的数据） 2. 产品序列号（赛门铁克分配给您产品的数据） 3. 诺顿帐号（赛门铁克生成的数据） 4. 文件路径 *5. 被识别为恶意软件的非可执行和可移植的可执行文件 6. 诺顿产品认为可能是欺诈性的已访问的网站的 URL 7. 在其计算机上安装下载的安全风险之前用户最近访问的网站的 URL 8. 关于在用户的设备上不时运行的进程和应用程序的信息，包括在遇到潜在安全风险时的信息 9. 在回应潜在安全风险时由用户的设备发送的数据样本	诺顿社区防卫是由赛门铁克在后端托管和管理的服务，收集的所有数据都按照以下方式传送给赛门铁克： 1. 机器 ID 用于跟踪每个订阅中使用产品的唯一设备的数量，以便审计和行使许可证权利和利益。 2. 产品序列号提供给每个用户，并用于确保每个产品获得赛门铁克的使用许可。 3. 诺顿帐号用来追踪订阅特定诺顿产品的用户数量。 4.-5. 捕获文件路径以及非可执行文件和可移植的可执行文件，用以帮助确定 影响或来自用户设备的网络威胁的来源和逻辑位置。 6.-7. URL 用于识别基于 web 的潜在安全风险来源，并提高赛门铁克产品与服务检测恶意行为、有害事件、欺诈网站、犯罪软件和其他形式的网络安全威胁的能力。 8.-9. 设备数据用于提高赛门铁克对网络威胁的知识和了解。设备数据也经过处理，以便在未来为赛门铁克产品与服务的用户提供更好的保护，并对网络安全趋势进行统计分析。

诺顿 Core

产品/服务描述	数据访问和收集	数据处理
诺顿 Core 是一种无线路由器，它能保护连接到路由器的设备免于恶意软件、病毒、黑客和其他网络威胁。	*1. 无线网络 SSID/密码（已加密） 2. 设备信息，包括在分配设备名称时用户包含的任何个人数据，并且，如果用户提供，还包括接受设备分配的人的姓名或别名，以及和设备用户代理数据/应用程序用户代理数据，包括设备类型、制造商和型号、操作系统和 IP 地址 3. 关于设备使用情况的数据，包括关于设备上次使用时间、每个已连接设备的互联网使用时间以及网络连接的网关日志的数据 4. 由用户定义和配置的父母控制信息和设置，包括被屏蔽的网站、访问网站、时间和内容过滤信息，以及被确定为或被认为是危险的网站的 URL *5. 用户创建诺顿帐户时可能提供的个人数据，包括用户名和可选图片 *6. 用户提供的用于客户支持和连接帮助的个人数据，如用户 ID、姓名、角色、用户特定的政策以及设备信息 7. 网络威胁遥测，包括试图下载恶意的可执行文件/移动应用程序的日志、其他危险事件或行为的记录，以及恶意软件样本等工件 *8. 用户联系信息、表达的偏好 *9. 送货地址及相关信息 10. 诺顿 Core 能够实现参与诺顿社区防卫	1. 为了用户自定义的 WiFi 网络配置而处理无线网络信息。 2. 为了许可证管理而处理设备信息，从而对设备及其流量进行分析，以监控路由器的健康和连接性，并协助调试、了解产品使用情况并对警报作出响应。 3. 处理设备使用数据是为了： • 优化诺顿 Core 的性能； • 告知用户站点安全性；以及 • 阻止浏览不安全的网站。 4. 父母控制信息和设置用于执行用户为其控制的配置文件定义的规则和策略、帮助用户检测与这些配置文件关联的个人数据的任何滥用以及与用户和控制的配置文件进行通信。 5.-6. 用户帐户信息由赛门铁克收集，以满足客户合同中概述的服务，并提供技术支持和帮助。 7. 网络威胁遥测信息被传输给赛门铁克，用于研究和开发，以改进赛门铁克的产品与服务，更好地保护用户的网络、设备、数据和身份。 8. 用户联系信息和偏好被传输给赛门铁克，目的是： • 在诺顿 Core 软件安装过程中指导用户； • 告知用户提升用户体验的方法； • 根据用户偏好（如语言和地理区域）向用户展示定制信息；以及 • 提高客户对于通过自有的和第三方呼叫中心提供的服务的满意度。 9. 送货地址和相关信息 是为了把诺顿 Core 硬件交付给用户。 10. 关于诺顿社区防卫的相关信息，请参阅本通知的诺顿社区防卫部分，了解更多详情。 此外，赛门铁克将使用源于收集的数据汇总的、去掉身份信息的、匿名的或其他非识别的数据（例如统计数据），目的是： • 进行整体网络安全研究； • 通过文件样本分析，改进对恶意软件和网络威胁的检测； • 跟踪和发布关于安全和身份盗用风险/趋势的报告； • 对产品部署进行统计分析，包括分析汇总用户群的趋势和比较； • 在可用性和响应时间方面监控和提升产品性能； • 了解与产品相关的沟通频率，以优化整体用户体验；以及 • 获取其他非用户特定的业务和市场洞察力，以提高我们的运营绩效。

诺顿移动安全

产品/服务描述	数据访问和收集	数据处理
，诺顿移动安全为受保护用户以及订阅者选择的设备提供防护，能让智能手机和平板电脑免受数字威胁，并能进行丢失或被盗设备恢复以及联系信息恢复	1. 受保护用户的移动设备数据，包括设备标识符（例如 IMEI、WiFi MAC 地址、UDID）、订阅者信息、手机号码和受保护用户的其他联系信息、设备名称/类型和制造商、操作系统类型和版本、无线运营商、网络类型、原产国、支持用例 ID、用户装机证书、来自设备的网站域名和相关 SSL 证书链以及 IP 地址 2. 使用数据，如下载和使用频率信息、日志数据和 cookie，以及关于用户如何连接到网络服务的网络服务信息 3. 每次产品执行扫描时，用户设备上的文件和应用程序的名称，包括目前不在赛门铁克的已知应用程序数据库中的被扫描的应用程序，用以保护用户免受恶意软件或危险功能的侵害，以及日历和 SD 卡的内容（可用时） 4. 网页浏览 URL、历史和书签 *5. 根据用户的选择，用户的设备上的联系人，包括通话和短信日志 6. 通话和设备音频设置 *7. 设备位置数据 *8. 产品也可以进行配置，从而如果拥有此类配备，并且在报告设备丢失或被盗的情况下，当设备继续被使用时、当输入不正确的密码而尝试解锁设备失败时或者当设备在关闭后被打开时，设备的前置摄像头就会拍一张照片 9. 移动设备上的数据的备份拷贝，包括联系人、通话记录、电话和短信	1. 处理移动设备数据、订阅者信息和受保护用户联系信息的目的包括： • 支持和优化产品性能； • 对赛门铁克的受保护用户身份进行身份验证； • 在软件安装过程中指导用户； • 与受保护用户沟通以提供服务； • 进行许可证管理；以及 • 提高客户对于通过自有的和第三方呼叫中心提供的服务的满意度。 2. 处理使用数据是为了：了解产品的使用和偏好，用以个性化和改善用户体验。 3. 处理文件、应用程序名称、日历（例如邀请中的 URL）和 SD 卡内容的目的是： • 警告用户潜在的有害应用程序； • 扫描设备是否存在恶意软件；以及 • 如果用户选择启用和执行产品的擦除命令，则从设备中清除个人内容。 4. 处理浏览数据的目的是： • 告知用户站点安全性； • 阻止浏览不安全的网站；以及 • 如果用户选择使用产品的 Web 保护功能或擦除命令，则擦除浏览历史和书签。 5. 处理用户设备上的联系信息（包括通话和短信日志）的目的是在用户选择的情况下提供通话/短信拦截功能。 6. 如果用户选择启用产品的拦截功能和/或 Scream 命令，手机设置可以阻止来自联系人的来电或修改设备的音频设置。 7. 8. 当设备丢失或被盗时，可以根据受保护用户的请求，收集设备位置和图像数据，以定位用户的设备。产品还可以向订阅者提供远程命令，用以在设备丢失或被盗时帮助定位受保护用户的设备。在某些情况下，当设备被报告丢失或被盗时，设备将被远程锁定。或者，当设备被报告丢失或被盗时，也可以随时关闭产品。在受保护用户许可的情况下，可以存储设备的最后 10 个已知位置的历史记录，以允许受保护用户跟踪设备的最近移动，即使该产品目前未被使用。 9. 如果用户选择使用备份数据，则会处理备份数据，以实现产品的备份和恢复功能。 此外，赛门铁克将使用源于收集的数据汇总的、去掉身份信息的、匿名的或其他非识别的数据（例如统计数据），目的是： • 进行整体网络安全研究； • 通过文件样本分析，改进对恶意软件和网络威胁的检测；

		• 跟踪和发布关于安全和身份盗用风险/趋势的报告； • 对产品部署进行统计分析，包括分析汇总用户群的趋势和比较； • 在可用性和响应时间方面监控和提升产品性能； • 了解与产品相关的沟通频率，以优化整体用户体验；以及 • 获取其他非用户特定的业务和市场洞察力，以提高我们的运营绩效。

诺顿安全扫描

产品/服务描述	数据访问和收集	数据处理
诺顿安全扫描提供对端点设备或用户选择的设备的扫描，识别潜在的问题或风险，并会向用户推荐产品和解决方案。	1. 机器 ID（赛门铁克内部生成的数据）；设备安装/卸载功能；设备信息和设备用户代理数据/应用程序用户代理数据，包括设备类型、OS 版本、OS 语言、制造商和型号；操作系统；以及相关的地理信息 2. 有关被扫描文件、用户体验以及被发现、修复和剩余的威胁的遥测信息；提交后的扫描日期和时间；关于安装和操作的状态信息（如果是在文件路径或文件夹名中，可能会附带个人数据）	1. 赛门铁克使用机器 ID 和相关信息的目的包括： • 在软件安装过程中指导用户； • 与用户沟通以提供服务； • 了解服务的使用和偏好，用以个性化和改善用户体验。 2. 赛门铁克使用遥测信息的目的包括： • 支持和优化服务性能；以及 • 研究和开发，以改进赛门铁克的产品与服务，更好地保护用户的网络、设备、数据和身份。 此外，赛门铁克将使用源于收集的数据汇总的、去掉身份信息的、匿名的或其他非识别的数据（例如统计数据），目的是： • 进行整体网络安全研究； • 通过文件样本分析，改进对恶意软件和网络威胁的检测； • 跟踪和发布关于安全和身份盗用风险/趋势的报告； • 对产品部署进行统计分析，包括分析汇总用户群的趋势和比较； • 在可用性和响应时间方面监控和提升产品性能； • 了解与产品相关的沟通频率，以优化整体用户体验；以及 • 获取其他非用户特定的业务和市场洞察力，以提高我们的运营绩效。

诺顿安全登录

产品/服务描述	数据访问和收集	数据处理
诺顿安全登录 (NSL) 是一个身份提供器，它提供了一种简单、安全、集中的方法来对用户进行身份验证。赛门铁克为各种诺顿产品的数百万用户提供了身份管理的基础设施。	*1. 用于协助认证用户身份的个人数据，如家庭住址、电话号码、出生日期及/或信用卡号码；用户的联系信息；用户可能输入到用户的诺顿账户的任何其他个人数据，或者用户可能为了客户支持和连接协助目的而提供的任何其他个人数据，如姓名和设备信息 2. 设备、产品与服务信息，以及设备用户代理数据/应用程序用户代理数据，包括设备类型；制造商；型号；操作系统和版本；设备信息和设备用户代理数据/应用程序用户代理数据，包括设备类型；制造商；型号；操作系统和版本；运行时间性能数据；已安装的应用程序；相关的地理信息、MAC 地址和 IP 地址 3. 关于互联网使用情况的使用数据，如被访问网站的 URL 和 IP 地址、搜索关键字和结果以及关于潜在安全风险的信息（包括被认为可能存在欺诈情况的网站的 URL 和 IP 地址，可能包含网站试图在未经用户许可的情况下获取的个人数据）	1. 赛门铁克处理个人数据的目的包括： • 为了赛门铁克或使用诺顿安全登录的信赖第三方，对赛门铁克用户的身份进行身份验证； • 签发身份证明和/或避免以用户名义进行的欺诈交易； • 在设置过程中指导用户； • 与用户沟通，以提供服务，包括支持和协助；以及 • 提高客户对于通过自有的和第三方呼叫中心提供的服务的满意度。 2. 赛门铁克处理设备、产品与服务信息的目的包括： • 支持和优化产品与服务性能； • 进行许可证管理；以及 • 了解产品的使用和偏好，用以个性化和改善用户体验。 3. 赛门铁克处理使用数据的目的包括： • 告知用户站点安全性； • 阻止浏览不安全的网站；以及 • 研究和开发，以改进赛门铁克的产品与服务，更好地保护用户的网络、设备、数据和身份。 此外，赛门铁克将使用源于收集的数据汇总的、去掉身份信息的、匿名的或其他非识别的数据（例如统计数据），目的是： • 进行整体网络安全研究； • 通过文件样本分析，改进对恶意软件和网络威胁的检测； • 跟踪和发布关于安全和身份盗用风险/趋势的报告； • 对产品部署进行统计分析，包括分析汇总用户群的趋势和比较； • 在可用性和响应时间方面监控和提升产品性能； • 了解与产品相关的沟通频率，以优化整体用户体验；以及 • 获取其他非用户特定的业务和市场洞察力，以提高我们的运营绩效。

诺顿 Ultimate Help-Desk 与诺顿 Computer Tune-Up

产品/服务描述	数据访问和收集	数据处理
诺顿终极帮助台 (Ultimate Help Desk) 使用户能联系专家，以协助解决从网络设置到设备诊断和故障排除等技术问题。 诺顿电脑调准 (Computer Tune-Up) 是诺顿 Ultimate Help Desk 内的一个功能，它使用诊断方式，帮助用户的设备像新的一样运行。	*1. 您通过电话向赛门铁克服务代表提供的请求信息，或者您在请求诺顿服务时在赛门铁克在线接口中输入的请求信息 2. 系统信息，包括：设备上使用的操作系统和浏览器的类型和版本；防火墙是否有效；杀毒软件是否安装、运行、更新；支持软件工具的内存和磁盘空间、代理配置和目录列表；浏览器信息，包括安全性和临时文件设置；设备上的活动端口、主机文件和网络接口设置；安装的程序和活动进程信息；应用程序和操作系统日志文件信息和注册表数据 3. 诊断信息，包括：被扫描的文件数量、被发现的威胁和被支持软件工具修复的威胁；被发现的威胁的类型；由支持软件工具确定的设备的安全状态（良好/一般/差）；未被支持软件工具修复的仍存在的威胁的数量和类型	1. 赛门铁克处理请求信息的目的包括： • 与用户沟通以提供服务； • 理解产品的使用和偏好，用以个性化和改善用户体验；以及 • 提高客户对于通过自有的和第三方呼叫中心提供的服务的满意度。 2. 赛门铁克处理系统信息的目的包括： • 交付用户请求的服务； • 支持和优化服务性能；以及 • 在使用服务期间指导用户； 3. 赛门铁克处理诊断信息的目的包括： • 告知用户所提供的服务的结果；以及 • 研究和开发，以改进赛门铁克的产品与服务，更好地保护用户的网络、设备、数据和身份。 此外，赛门铁克将使用源于收集的数据汇总的、去掉身份信息的、匿名的或其他非识别的数据（例如统计数据），目的是： • 进行整体网络安全研究； • 通过文件样本分析，改进对恶意软件和网络威胁的检测； • 跟踪和发布关于安全和身份盗用风险/趋势的报告； • 对产品部署进行统计分析，包括分析汇总用户群的趋势和比较； • 在可用性和响应时间方面监控和提升产品性能； • 了解与产品相关的沟通频率，以优化整体用户体验；以及 • 获取其他非用户特定的业务和市场洞察力，以提高我们的运营绩效。

诺顿防护 VPN(原：诺顿 WiFi 隐私)

产品/服务描述	数据访问和收集	数据处理
诺顿防护 VPN 通过对用户的信息进行加密以及保护用户的隐私来保护用户的设备以及保障用户的数据。	1. 订阅者信息和移动设备数据，包括设备名称、类型、OS 版本和语言； 2. 总带宽使用情况； 3. 临时使用数据，以帮助排除服务问题。	1. 赛门铁克处理订阅者信息和移动设备数据的目的包括： • 支持和优化服务性能； • 理解产品的使用和偏好，用以个性化和改善用户体验； • 在安装软件和使用服务过程中指导用户； • 与用户沟通以提供服务； • 提醒用户保护用户正在传输的信息；以及 • 提高客户对于通过自有的和第三方呼叫中心提供的服务的满意度。 2. 赛门铁克处理带宽使用数据是为了计费、网络操作和提供支持。 3. 赛门铁克处理临时使用数据的目的包括： • 选择最适合连接的服务器；以及 • 研究和开发，以改进赛门铁克的产品与服务，更好地保护用户的网络、设备、数据和身份。 在使用诺顿防护 VPN 过程中，我们通过赛门铁克的网络路由用户的互联网流量，这是一个“没有日志”的网络。这意味着在用户连接到诺顿防护 VPN 时，赛门铁克不会存储用户的原始 IP 地址，因此赛门铁克不能识别个人。赛门铁克基于规则的自动流量管理可能需要对互联网数据流量进行实时分析，包括目标网站或 IP 地址和原始 IP 地址，但不会维持关于此类信息的日志。赛门铁克不存储用户下载、使用或访问的应用程序、服务或网站的信息。正如赛门铁克 - 诺顿全球隐私声明中解释的那样，由于赛门铁克管理一个全球网络，因此用户的互联网流量可以通过一个或多个不同的国家路由。 此外，赛门铁克将使用源于收集的数据汇总的、去掉身份信息的、匿名的或其他非识别的数据（例如统计数据），目的是： • 进行整体网络安全研究； • 通过文件样本分析，改进对恶意软件和网络威胁的检测； • 跟踪和发布关于安全和身份盗用风险/趋势的报告； • 对产品部署进行统计分析，包括分析汇总用户群的趋势和比较； • 在可用性和响应时间方面监控和提升产品性能； • 了解与产品相关的沟通频率，以优化整体用户体验；以及 • 获取其他非用户特定的业务和市场洞察力，以提高我们的运营绩效。

诺顿安全产品（安全、互联网安全、One、防病毒、360）

本部分包括诺顿安全（标准版、豪华版和高级版）、诺顿网络安全、诺顿 One、诺顿防病毒、诺顿防病毒入门版、诺顿 360、诺顿 360PE 和诺顿 360MD。

产品/服务描述	数据访问和收集	数据处理
诺顿安全产品提供端点安全保护，以防御勒索软件、病毒、间谍软件、恶意软件和其他在线威胁。	1. 订阅者信息和设备数据，包括用户为了创建诺顿账户而可能输入的*个人数据，如用户名和可选图片；用户在分配设备名称时所包括的任何*个人数据，以及可能提供的设备被分配给的人的姓名或别名，还有设备用户代理数据/应用程序用户代理数据，包括设备类型、制造商和型号；操作系统和版本；应用程序和版本；相关地理信息、MAC 地址、机器 ID、IP 地址；关于安装和操作的状态信息，如果是文件或文件夹名称，那么可能包括附带的个人数据；用户为了客户支持和连接帮助而向赛门铁克提供的任何其他个人数据，如用户 ID、姓名、角色、政策和设备信息 2. 关于互联网使用情况的数据，如被访问网站的 URL 和 IP 地址、搜索关键字和结果以及关于潜在安全风险的信息（包括被认为可能存在欺诈情况的网站的 URL 和 IP 地址，可能包含网站试图在未经用户许可的情况下获取的个人数据） 3. 关于设备使用和诊断的数据，包括：有关设备使用上次时间、每个已连接设备的互联网使用时间以及详细记录网络连接活动的网关日志的数据；被识别为潜在恶意软件的可执行文件，其中可能包括恶意软件未经用户许可获取的个人数据；发送给赛门铁克的、用户允许报告为垃圾邮件或被错误识别为垃圾邮件的电子邮件；“崩溃转储”信息，或当产品与服务遇到问题时用户可能选择向赛门铁克发送的报告中包含的信息，其中可能包括系统语言、国家语言环境、操作系统以及在错误时运行的进程/文件 4. 由用户定义和配置的父母控制信息和设置，包括屏蔽的网站、访问的网站、时间和内容过滤信息，以及被确定为或被认为是危险的网站的 URL。	1. 赛门铁克处理订阅者信息和设备数据的目的包括： • 支持和优化产品与服务性能； • 对赛门铁克用户的身份进行身份验证； • 理解产品的使用和偏好，用以个性化和改善用户体验； • 在软件安装过程中指导用户； • 与用户沟通以提供服务； • 进行许可证管理；以及 • 提高客户对于通过自有的和第三方呼叫中心提供的服务的满意度。 2. 处理互联网使用数据的目的包括： • 告知用户站点安全性；以及 • 阻止浏览不安全的网站。 3. 赛门铁克处理设备使用和诊断数据的目的包括： • 了解产品使用情况； • 提供产品与服务的保护功能；以及 • 研究和开发，以改进赛门铁克的产品与服务，更好地保护用户的网络、设备、数据和身份。 4. 父母控制信息和设置用于执行用户为其控制的配置文件定义的规则和策略、帮助用户检测与这些配置文件关联的个人数据的任何滥用以及与用户和控制的配置文件进行通信。 此外，赛门铁克将使用源于收集的数据汇总的、去掉身份信息的、匿名的或其他非识别的数据（例如统计数据），目的是： • 进行整体网络安全研究； • 通过文件样本分析，改进对恶意软件和网络威胁的检测； • 跟踪和发布关于安全和身份盗用风险/趋势的报告； • 对产品部署进行统计分析，包括分析汇总用户群的趋势和比较； • 在可用性和响应时间方面监控和提升产品性能； • 了解与产品相关的沟通频率，以优化整体用户体验；以及 • 获取其他非用户特定的业务和市场洞察力，以提高我们的运营绩效。

诺顿安全搜索、诺顿主页、诺顿安全网页

产品/服务描述	数据访问和收集	数据处理
诺顿安全搜索是一个搜索引擎网站，它通过过滤搜索结果和为用户提供网站安全评级，以提供更安全的网页浏览体验，从而保护用户免受不安全网站的侵害。它也是一种浏览器扩展，提供了访问诺顿安全搜索网站的各种方法。这个扩展的不同版本可以根据用户： a) 将浏览器的默认搜索引擎重写为诺顿安全搜索网站； b) 将浏览器默认的搜索引擎设置重写为诺顿安全搜索网站，并把浏览器的默认主页和新选项卡重写为诺顿主页。 诺顿主页是一种浏览器扩展和能够启用诺顿安全搜索网站的默认主页。 诺顿安全网页是用户选择使用的浏览器扩展，以监视浏览活动和网页内容。它使用信誉服务和网页内容分析来帮助保护用户免受恶意网站内容、网络钓鱼和其他威胁。	1. 订阅者信息、设备和软件数据，包括：网页浏览器名称、版本和首选语言；操作系统、版本或平台；用户设备的 IP 地址 2. 服务使用数据，包括：社交媒体和网络邮件中的链接；网站浏览活动；网页搜索条件；诺顿产品管理的不同搜索框中的默认输入；搜索引擎结果 3. 在诺顿安全搜索网站和诺顿主页网站上放置的 cookie、像素标签、脚本或类似的技术	1. 赛门铁克处理订阅者信息以及设备和软件数据的目的包括： • 支持和优化服务性能； • 进行许可证管理； • 理解产品的使用和偏好，用以个性化和改善用户体验； • 在软件安装过程中指导用户； • 提供产品与服务的增强功能，更好地保护用户、用户的网络、设备、数据和标识；以及 • 提高客户对于通过自有的和第三方呼叫中心提供的服务的满意度。 2. 赛门铁克以及代表赛门铁克处理服务使用数据的目的是： • 告知用户站点安全性； • 阻止浏览不安全的网站；以及 • 分析服务使用。 通过我们的诺顿安全搜索产品进行的用户搜索查询请求将被指向我们的第三方搜索伙伴 Oath/Yahoo!（针对美国和加拿大）和 IACI（针对非美国/加拿大），以便将查询研究交付给您。我们的第三方合作伙伴也可能根据您在诺顿安全搜索中的活动直接从您那里收集信息。我们的第三方合作伙伴将作为数据控制者收集这些数据，以便处理您的搜索查询。此类数据收集受到第三方合作伙伴的隐私政策、声明和通知的约束。 为了将诺顿安全搜索交付给您，您的搜索查询请求将被指向我们的第三方合作伙伴（即不是赛门铁克的公司），在那里，第三方合作伙伴将处理您的请求。第三方合作伙伴也可能通过您在诺顿安全搜索上的活动直接向您收集信息（统称“第三方数据”）。第三方合作伙伴将是数据控制者，用于处理您的搜索查询，因此，将由我们的第三方合作伙伴而不是赛门铁克决定如何收集、使用、公开、保留或处理第三方数据。您的第三方数据以第三方合作伙伴的隐私声明为准，以便为了执行搜索查询而处理您的数据。请参阅我们的第三方合作伙伴隐私声明。 3. 处理 cookie 和类似的跟踪器的目的是为了遵循功能使用偏好和历史。有关 cookie 的更多信息，请参见赛门铁克 - 诺顿全球隐私声明中的标题为“追踪技术、cookie 和禁止追踪”的部分。 匿名化的 IP 地址和产品使用信息通过 Google Analytics 的测量协议进行处理，以达到关键错误统计分析和管理的目的。请点击这里，获取关于 Google Analytics 数据保障的信息。 此外，赛门铁克将使用源于收集的数据汇总的、去掉身份信息的、匿名的或其他非识别的数据（例如统计数据），目的是： • 进行整体网络安全研究； • 通过文件样本分析，改进对恶意软件和网络威胁的检测； • 跟踪和发布关于安全和身份盗用风险/趋势的报告； • 对产品部署进行统计分析，包括分析汇总用户群的趋势和比较；以及 • 在可用性和响应时间方面监控和提升产品性能；

诺顿安全工具栏

产品/服务描述	数据访问和收集	数据处理
诺顿安全工具栏有两种变体，a) 一种是微软 Internet Explorer 的附加组件，b) 另一种是谷歌 Chrome 的浏览器扩展。用户可以使用这两种变体来监视用户的浏览活动和 web 页面内容。他们使用信誉服务和网页内容分析来帮助保护用户免受恶意网站内容、网络钓鱼和其他威胁。 Internet Explorer 变体能够实现在浏览器用户界面中访问和使用诺顿密码管理器库信息。它还提供一个搜索框，用以在诺顿安全搜索网站上进行搜索。谷歌 Chrome 变体也提供一个搜索框，用以在诺顿安全搜索网站上进行搜索。	1. 设备和软件数据，包括：网页浏览器名称、版本和首选语言；操作系统、版本或平台；用户设备的 IP 地址 2. 产品使用数据，包括：网站浏览活动；受限制的网站浏览历史；网页搜索条件；诺顿产品管理的不同搜索框中的默认输入；搜索引擎结果 3. 在诺顿安全搜索网站和诺顿主页网站上放置的 cookie、像素标签、脚本或类似的技术	1. 赛门铁克处理设备和软件数据的目的包括： • 支持和优化服务性能； • 进行许可证管理； • 理解产品的使用和偏好，用以个性化和改善用户体验； • 在软件安装过程中指导用户； • 提供产品与服务的增强功能，更好地保护用户、用户的网络、设备、数据和标识；以及 • 提高客户对于通过自有的和第三方呼叫中心提供的服务的满意度。 2. 赛门铁克以及代表赛门铁克处理产品使用数据的目的是： • 告知用户站点安全性； • 阻止浏览不安全的网站；以及 • 分析服务使用。 3. 处理 cookie 和类似的跟踪器的目的是为了遵循功能使用偏好和历史。有关 cookie 的更多信息，请参见赛门铁克 - 诺顿全球隐私声明中的标题为“追踪技术、cookie 和禁止追踪”的部分。 此外，赛门铁克将使用源于收集的数据汇总的、去掉身份信息的、匿名的或其他非识别的数据（例如统计数据），目的是： • 进行整体网络安全研究； • 通过文件样本分析，改进对恶意软件和网络威胁的检测； • 跟踪和发布关于安全和身份盗用风险/趋势的报告； • 对产品部署进行统计分析，包括分析汇总用户群的趋势和比较；以及 • 在可用性和响应时间方面监控和提升产品性能；

诺顿密码管理器 (原：诺顿身份安全)

产品/服务描述	数据访问和收集	数据处理
诺顿密码管理器有两个变体：a) 诺顿安全的一个组成部分，以及 b) 针对所有主要浏览器（Internet Explorer 除外）的浏览器扩展。所有变体都是一个密码管理器，用于管理用户名、密码和其他用于执行在线活动的信息。	1. 订阅者信息、设备和软件数据，包括：web 浏览器名称、版本和首选语言；操作系统、版本或平台；用户设备的 IP 地址；用户披露的*其他个人数据，包括用户名、密码、网址、物理地址、付款账号、过期信息和自由格式文本 2. 服务使用数据，包括；网站浏览活动；网页搜索条件；诺顿产品管理的不同搜索框中的默认输入；搜索引擎结果	1. 赛门铁克处理设备和软件数据的目的包括： • 支持和优化服务性能； • 进行许可证管理； • 理解产品的使用和偏好，用以个性化和改善用户体验； • 在软件安装过程中指导用户； • 提供产品与服务的增强功能，更好地保护用户、用户的网络、设备、数据和标识；以及 • 提高客户对于通过自有的和第三方呼叫中心提供的服务的满意度。 2. 赛门铁克以及代表赛门铁克（的员工）处理产品使用数据的目的是： • 告知用户站点安全性； • 阻止浏览不安全的网站；以及 • 分析服务使用。 匿名 IP 地址和产品使用信息通过 Google Analytics 的测量协议进行处理，以达到关键错误统计分析和管理的目的。请点击这里，获取关于 Google Analytics 数据保障的信息。 此外，赛门铁克将使用源于收集的数据汇总的、去掉身份信息的、匿名的或其他非识别的数据（例如统计数据），目的是： • 进行整体网络安全研究； • 通过文件样本分析，改进对恶意软件和网络威胁的检测； • 跟踪和发布关于安全和身份盗用风险/趋势的报告； • 对产品部署进行统计分析，包括分析汇总用户群的趋势和比较；以及 • 在可用性和响应时间方面监控和提升产品性能；

诺顿 Family Premier

产品/服务描述	数据访问和收集	数据处理
诺顿家长控制软件 (Family Premier) 能通过用户定义和订阅者管理的保护设置和特性，帮助保护受保护用户以及订阅者选择使用父母控制来进行保护的设备。 有关诺顿 Family Premier 的其他细节，请参阅下面的“诺顿 Family Premier 附加信息”一节	*1. 订阅者信息，例如：管理员联系信息，包括但不限于订阅者的姓名、电子邮箱地址和密码，用以保护订阅者的帐户；用户在配置服务或任何其他后续服务调用时提供的个人数据； 2. 设备和软件数据，包括：诺顿 Family 客户端软件在订阅者或受保护用户设备上的安装状态；软件配置、产品细节及安装状态；许可证状态、许可证授权信息、许可证 ID 和许可证使用情况；设备名称、类型、OS 版本、语言、位置（全球定位系统，GPS）、浏览器类型和版本；设备硬件、软件和应用程序清单；应用程序和数据库访问配置、政策需求和政策合规状态，以及应用程序异常和工作流故障日志； *3. 订阅者选择向赛门铁克披露的受保护用户信息，包括：姓名、性别、年龄和出生年份；头像；与受保护用户有关的官方身份证号（例如：社会保险号码、国民身份证号码）的最后六位数字、电子邮箱地址、手机号码、学校名称或用户想要保护的其他信息；机器登录帐户详细信息、国家和时区； 4. 订阅者指示赛门铁克监控的受保护之用户网络活动信息，根据每名用户的全权选择，包括：在线和移动设备的活动和位置；受保护用户试图访问的网站和产品阻止受保护用户访问的网站；受保护用户使用的在线搜索词；受保护用户在其设备上安装或卸载的应用程序（当订阅者已经激活应用程序监控时）；受保护用户的设备使用时间；*受保护用户的配置文件名称、配置文件 URL、年龄、Facebook 配置文件 ID 和访问的视频；受保护用户在 YouTube.com 和/或 Hulu 上观看的视频（当用户已激活视频监控时）。	1. 赛门铁克处理订阅者信息的目的是： • 支持和优化诺顿 Family 的性能； • 提供支持或排除故障协助； • 根据订阅者的许可或在适用法律允许的情况下，给订阅者发送促销信息；以及 • 设置订阅者的诺顿帐户。 2. 赛门铁克处理设备和软件数据的目的包括： • 确保产品的正常运作，并提供订阅者所要求的服务； • 进行许可证管理； • 评估和改进产品的安装成功率； • 研究和开发，以改进赛门铁克的产品与服务，更好地保护订阅者和受保护用户的网络、设备、数据和身份； 3. 处理受保护用户的信息的目的包括： • 让赛门铁克识别并认证订阅者和受保护用户； • 帮助订阅者检测受保护用户个人数据的任何滥用；以及 • 与用户通信，并根据订阅者的许可，与受保护用户进行通信，以提供服务。 4. 处理受保护用户活动信息的目的包括： • 帮助订阅者监督受保护用户设备的在线活动； • 限制安装的恶意软件造成的损害； • 协助执行订阅者定义的、关于受保护用户设备线上活动的规则； • 使订阅者能够检测受保护的用户是否通过在线或短信/彩信通信受到威胁；以及 • 帮助订阅者保护受保护用户免受此类威胁。 此外，赛门铁克将使用源于收集的数据汇总的、去掉身份信息的、匿名的或其他非识别的数据（例如统计数据），目的是： • 进行整体网络安全研究； • 通过文件样本分析，改进对恶意软件和网络威胁的检测； • 跟踪和发布关于安全和身份盗用风险/趋势的报告；以及 • 对产品部署进行统计分析，包括分析汇总用户群的趋势和比较。

诺顿 Family Premier 附加信息

如果订阅者选择激活该服务，那么诺顿 Family 将不允许受保护用户将其个人数据公开。

在订阅者所在国家或地区的适用法律允许的情况下，赛门铁克可能提供**短信监管**服务，让用户来拦截或监控受保护用户的手机收发的短信 (SMS) 和彩信 (MMS)，以及**位置监控服务**。适用于订阅者的当地法律可能会限制或禁止监控 SMS 和 MMS 的交换和/或位置，以及使用任何此类监控记录。订阅者在激活该功能之前，必须先向当地有权机关查询。

当订阅者启用位置监控服务时，诺顿 Family 将执行订阅者的指令，使用 GPS 跟踪和收集订阅者指定移动设备的地理定位。为了让诺顿 Family 追踪、收集、使用或披露指定设备的地理定位，需要订阅者的同意以及移动设备用户的同意，或者对该用户承担父母责任的人员的同意（视情况而定）。相关同意是通过诺顿在线门户网站收集的，或者是位于产品中（视情况而定），并在用户向赛门铁克在线购买此类服务时输入他们的支付卡信息时确认同意。您可以随时撤销您提供的任何同意。如需关于如何做到这一点的更多信息，请参阅赛门铁克 - 诺顿全球隐私声明中**"您的隐私权"部分**。服务终止后，赛门铁克将删除与此服务有关的订阅者帐户信息。

一旦订阅者在指定的移动设备上下载应用程序，赛门铁克就会收集该设备的地理定位，即使应用程序未在使用中。我们将只向订阅者公开这些地理定位信息，以便订阅者能够定位设备，并且我们处理此类信息将只用于操作目的，用以提供订阅者所请求的服务和功能。订阅者不得使用该产品的位置监控服务来监控涉及订阅者不承担父母责任的个人的数据、位置、活动或任何其他方面。欧洲经济区的订阅者在承担父母责任的情形下应与受保护用户进行交谈，特别是在他们超过 13 岁的情况下，并采取一切必要措施以确保受保护用户了解订阅者对产品和相关服务的使用权利。当选择使用产品和相关服务时，订阅者只负责遵守适用于订阅者与受保护用户的关系以及对受保护用户的父母责任的所有法律和规则。

短信监控

默认情况下，短信监控会被关闭。订阅者必须单独打开短信监控功能，并将诺顿 Family 安装到指定进行监控的移动设备上。当激活时，短信监控将从指定设备收集以下信息：

- 被监控设备的手机号码以及与设备交换 SMS 和 MMS 的其他设备的手机号码；
- 由指定的设备接收或发送的 SMS 消息的内容（对于 MMS 交换，赛门铁克不会记录或捕获交换的任何多媒体内容，只记录发生 MMS 交换的事实）；
- 在可用的情况下，在指定设备上与将 SMS 和 MMS 通信发送给指定的设备或接收来自该设备的通信的移动电话号码相关联的通讯录名称；
- 对话的日期/时间戳；
- 指定设备的位置；
- 被拦截 SMS/MMS 消息的事件日志，（包括双方的电话号码）和相关的名称（当在指定设备的通讯录中可用时）。

开始监控订阅者指定的移动设备发送和/或接收的 SMS 或 MMS 消息之前，赛门铁克将把 SMS 警报发送到指定的设备上，提醒设备用户，产品将执行订阅者的指令，记录和监控指定设备上交换的 SMS 或 MMS 的内容。如果在收到此短信提醒后，SMS 或 MMS 消息的交换继续在指定的设备上进行，则本通知中所述的短信记录和监控将按照订阅者的指示开始。赛门铁克将在一个月或每一次有新的对话时，向指定设备重申相同的短信提醒。

如果订阅者选择拦截与特定发送方进行的所有 SMS 或 MMS 消息，我们就会通知指定设备的用户，并向对应的发送方发送一条消息，指示消息被拦截，消息无法传递。