隐私数据表

由北京神州数码云计算有限公司运营的 Cisco Secure Access China

本隐私数据表介绍了由北京神州数码云计算有限公司运营的 Cisco Secure Access China (“Secure Access China”) 对个人数据（或可识别个人身份信息）的处理。

Secure Access China 是一款由北京神州数码云计算有限公司（“神州云计算”）运营的基于云的安全解决方案，供订阅了 Secure Access China 云服务的公司或个人使用。神州云计算基于 Cisco International Limited（“思科”）向其许可的技术提供 Secure Access China。服务的底层技术由思科及其关联方开发和维护，但中国国内服务由神州云计算运营并向中国大陆境内用户提供使用。

神州云计算将以符合本隐私数据表的方式处理来自 Secure Access China 的个人数据。神州云计算是为管理和维护客户关系而处理个人数据的个人信息处理者，也是为提供 Secure Access China 的功能而处理个人数据的个人信息处理者。

1. 概述

Secure Access China 是一款云安全服务边缘解决方案，旨在允许用户从位于中国大陆的任何设备安全地连接到互联网和私有应用程序。

Secure Access China 也可与第三方产品集成，包括通过 Cisco Security Cloud Control（开通和订阅管理）和 Cisco Secure Client（连接）提供的思科原厂产品功能。Cisco Secure Client 收集的数据见本隐私数据表所示。有关个人数据处理的信息，请访问思科信任门户，参阅 Security Cloud Control 的隐私数据表。对于脱离神州云计算控制范围用于非神州云计算产品的客户数据，神州云计算概不负责。相关第三方系统内数据的保护受相关第三方的合同和政策的约束。

请参阅 Cisco Secure Access China，了解更多信息。

2. 个人数据处理

表 1 列出了 Secure Access China 为提供服务而处理的个人数据，并说明了处理这些数据的原因。

表 1

个人数据类别	所处理的个人数据的类型	处理目的
账户数据	• 控制面板/控制台用户（均称为 “管理员”）的名字和姓氏 • 管理员电子邮箱地址 • 公司名称、街道、城市、州/省/地区、国家、电话号码 • 管理员 IP 地址	• 激活、维护、支持和改进服务 • 账单、发票和税务合规 • 出口合规 • 通知功能和其他更新 • 身份验证和授权 • 管理授权和续约

连接数据 **（VPN 即服务、漫游）**	• 设备私有和/或公共 IP 地址 • 用户 ID 和/或用户名 • 用户组 ID • 设备 ID • 设备名称 • 硬件 UUID • 目标私有应用信息（应用 ID、IP、FQDN） • 设备安全态势数据（见下文） • 网络流量 (HTTP/HTTPS) 中包含的个人数据，包括报头、URL 和 Cookie • 组织 ID • Active Directory (AD) 或身份提供商(IdP) GUID/ UPN（如果配置了本地 AD/云 IdP）	• 提供、维护、支持和改进服务 • 启用与互联网和私有应用的安全连接
设备安全态势数据	• 设备公共 IP 地址 • 用户 ID • 设备公钥 • 设备标识符（例如，设备 ID、设备/主机名、计算机 GUID） • 设备操作系统和版本 • 设备配置属性（例如，是否设置密码、是否已启用磁盘加密、是否已启用屏幕锁定） • WiFi 指纹（设备位置快照，用捕获时通过可见 SSID 得出的哈希值表示）	• 提供、维护、支持和改进服务 • 评估并验证设备的安全和状态，以确定是否应向设备授权以连接至网络或私有应用
安全数据	**安全 Web 网关**[1]	
	• 网络流量中包含的个人数据（例如，报头、URL、正文内容）[2] • 源和目标 IP 地址 • 来源 ID • 组织 ID • 设备 ID • 时间戳 • 代理特定报头 • 与用户或设备关联的云应用 • 所检查的文件中的个人数据	• 提供、维护、支持和改进服务 • 提供 URL 和文件级别的精细保护
	防火墙即服务	
	• 组织 ID • 私有和/或公共源及目标 IP 地址 • 应用 ID (公共/私有) • 用户 ID • 数据包内容（用于 IPS<入侵防御系统>功能）	• 提供、维护、支持和改进服务 • 提供 URL 和文件级别的精细保护
	数据丢失防护 (DLP)[1]	

[1] 神州云计算不会将身份数据（例如，active Directory、IdP、Google Workspace ID、用户名、用户 ID 以及“配置数据”中所述的其他身份信息）与此功能的事件日志一起存储。产品在仪表板中显示时，会将身份数据与事件日志进行配对，以便使用报告 API 进行报告，以及在客户选择 S3 导出选项的情况下将事件日志导出到客户特定的 AWS S3 存储桶。

[2] 系统不会记录 HTTPS 的 URL 查询参数，但客户可以选择将完整的 URL 导出到 S3 存储桶。

	实时 DLP • 文件名 • 文件 ID • 所扫描的 SaaS 环境中的个人数据、消息、文件以及其他通过 DLP 检查的内容 • 触发违规的文本片段及周围文本 • 在进行相关配置的情况下通过 AD/IdP 获取的用户身份数据 • 实时 DLP 会扫描出站和某些入站流量，以及此类流量中包含的任何个人数据。有关实时 DLP 入站和出站扫描的更多信息，请参阅 Secure Access China 用户指南	• 提供、维护、支持和改进服务 • 通过实时 DLP 的 Secure Access China 服务，在传输中的文件、消息和其他客户内容中发现、监控敏感信息（包括个人数据）并对敏感信息采取措施（例如，屏蔽）
	云应用发现	
	应用发现根据所支持的网络数据源导入的网络流量日志，其中可能包括： • 用户 ID 和/或电子邮箱地址 • 用户的名字和姓氏 • 源 IP 地址和关联的云应用 • 目标 URL	• 提供、维护、支持和改进服务 • 检测用户使用的云应用并提供风险评分
控制平面数据（配置、策略、身份）	配置和策略数据	
	• 审计日志，其中包括管理员名称 • 策略设置，其中包括管理员名称和 IP 地址 • 对象标签（例如，漫游设备和移动设备名称） • Chromebook 客户端邮件 ID 和/或设备序列号和操作系统 • 唯一账户 ID（例如组织 ID） • 控制面板内生成的报告中的任何个人数据（报告从存储在美国和欧盟的事件日志存储内的事件日志中提取数据）	• 处理配置信息以记录实施和/或更改的策略以及进行更改的客户管理员 • 提供与账户相关的信息 • 提供管理员请求的报告
	用户和设备身份数据	
	• 如果使用 AD 或 IdP 附加组件：AD/IDP 用户和设备身份（名字、姓氏、用户名、显	• 管理策略并精确定位每个用户或设备的活动以提供服务 • 对用户和/或设备进行身份验证

	示名称、电子邮箱、组名称、设备 ID、设备名称、用户 ID、组 ID）[3] • 源 IP 地址 • 用户主体名称 (UPN) • 设备主机名 • 设备密钥（设备 ID 格式取决于设备，例如，对于 Chromebook，设备 ID 格式是用户的电子邮箱或 ID 或者设备的序列号） • 设备序列号和操作系统 • Google Workspace ID（如果使用 Google Workspace 集成）	
支持数据	• 姓名 • 电子邮件 • 被指定打开支持故障单的员工的电话号码 • 身份验证信息（不包括密码） • 工作机构和职责 • 客户提供的案例附件数据（包括文本、音频、视频或图像文件）神州云计算不会故意通过客户案例附件收集或处理个人数据。客户应提供尽可能少的个人数据。但是，客户提供的文件中可能包含未经请求的个人数据。	• 提供远程访问支持 • 审查支持服务的质量 • 对服务解决方案进行分析

Cisco Secure Access 收集 “系统信息” 是为了帮助神州云计算了解产品使用情况，从而改进和采用相关产品。作为此类系统信息的一部分进行处理的任何个人数据都会受到相应保护。

3. 数据中心地点

Secure Access China 使用中国的 AWS 数据中心用于 Secure Access China 配置、策略、报告和控制平面（统称为 “控制平面”）以及数据处理，从而确保安全性和实施客户策略（统称为 “数据平面”）。请参阅下表和下文中的其他详细信息。

3.1 数据处理

表 2

服务	数据中心地点
• 账户数据 • 控制平面数据（配置、策略、身份） • 连接数据（VPN 即服务、漫游） • 设备安全评估数据 • 安全 Web 网关 • 防火墙即服务 • 实时 DLP	中国大陆地区

[3] 系统不会记录 HTTPS 的 URL 查询参数，但客户可以选择将完整的 URL 导出到 S3 存储桶。
如果使用随 Secure Access China 产品提供的用户管理服务，通过 Google 的 API 来集成 Google Workspace 身份，则神州云计算将根据 Google API 服务用户数据政策（包括 “限制使用” 要求）处理从 Google 收到的数据。

• 云应用发现 • 支持数据	

Cisco Security Cloud Control (SCC) 和 Cisco Secure Client是您使用 Secure Access China 订阅中的思科产品（非神州云计算产品）。对于 SCC，客户个人数据（例如，管理员用户名、电子邮箱地址）将在美国进行处理和存储。有关更多信息，请访问思科信任门户，参阅 Security Cloud Control 的隐私数据表。有关其他少数将数据发送到中国境外的情况，请参阅第 8 节（受托处理个人数据的第三方[XD1]）。对于 Cisco Secure Client，客户必须选择退出客户体验模块，以防止其数据被发送到中国境外。有关选择退出说明，请参阅 Secure Access China 产品文件。

3.2 数据存储

（在启用日志记录的情况下）数据平面使用和事件数据（“事件日志”）以及控制平面数据被存储在第 6 节中引用的位置处。对于大多数事件日志，客户可以选择不记录任何内容、记录所有内容或仅记录安全数据。有关日志记录的详细信息，请参阅 Secure Access China 产品文件。入侵防御 (IPS) 的日志记录始终处于启用状态。

4. 跨境数据传输机制

如果您在中国大陆地区使用由神州云计算运营的 Secure Access China 服务和/或使用神州云计算的技术支持，则您在使用服务期间生成的所有个人数据都将存储在中华人民共和国境内，存储的范围和详细信息见第 3 节和第 8 节所述，并且此类存储和传输行为均符合中华人民共和国相关法律法规的要求。应当明确指出的是，如果神州云计算要解决您在使用产品/服务的过程中出现的技术问题或如果是为了产品的正常运行，并且需要将客户的使用数据和必要的个人信息传输至境外，则神州云计算将确保此类传输符合中国法律法规的规定。如果您不希望将您在使用 Secure Access China 产品和服务期间生成的必要的个人信息传输至境外，则您将无法使用此类产品。

5. 访问控制

下表列出了 Secure Access China 为履行服务而使用的个人数据、谁可以访问此类数据以及为何访问此类数据的信息。

表 3

个人数据类别	谁有访问权限[4]	访问目的
账户数据	经授权的神州云计算和思科员工	开通客户账户；账单/发票和税务合规；出口合规；在相应数据访问和安全控制措施的约束下为服务提供支持
	客户管理员	输入、修改、控制管理员数据
连接数据 **（VPN 即服务、漫游）**	经授权的神州云计算和思科员工	在相应数据访问和安全控制措施的约束下提供、支持、维护和改进服务
	客户管理员	在 UI 中以及通过报告查看数据。可以通过选择数据导出选项，将数据导出至 S3

[4] 对于连接数据、设备安全评估数据、安全数据和控制平面数据，从策略角度来看，神州云计算不会访问此类数据，但是，由于神州云计算具有根访问权限，因此神州云计算有能力访问此类数据。

设备安全态势数据	经授权的神州云计算和思科员工	在相应数据访问和安全控制措施的约束下提供、支持、维护和改进服务
安全数据	经授权的神州云计算和思科员工	提供、支持、维护和改进服务
	客户管理员	在 UI 中以及通过报告查看数据。可以通过选择数据导出选项，将数据导出至 S3
控制平面数据（配置、策略、身份）	经授权的神州云计算和思科员工	在相应数据访问和安全控制措施的约束下提供、支持、维护和改进服务
	客户管理员	管理和配置账户，制定和维护策略
支持数据	经授权的神州云计算和思科员工	与客户合作解决其支持案例
	客户	与神州云计算合作解决其支持案例

6. 数据保留

下表列出了 Secure Access China 使用的个人数据、需要保留此类数据的时长、我们保留此类数据的原因以及保留位置的信息。

表 4

个人数据类别	所处理的个人数据的类型	保留期和保留位置[5]	保留的目的
账户数据	请参阅表 1	按需删除（中国大陆地区）	为合法商业目的而保留管理数据
连接数据（VPN 即服务、漫游）	管理服务日志： • 请参阅表 1（不包括设备安全态势数据中的 WiFi 指纹）	最多 90 天（中国大陆地区）	对服务配置和系统错误进行故障排除
	事件日志： • 设备公用/专用 IP 地址 • 用户 ID • 组织 ID • 用户组 ID • 设备 ID • 目标私有应用信息 • 设备操作系统和版本 • 设备配置属性 • 地理位置（根据公共 IP 地址得出）	最多 31 天（中国大陆地区）	持续的功能使用情况和报告；故障排除
设备安全态势数据	应用程序日志： 请参阅表 1（不包括 WiFi 指纹）	最多 90 天（中国大陆地区）	故障排除和调试

[5] 在系统崩溃的情况（这种情况不太可能发生）下，会自动捕获崩溃时存储器中所存储的数据（“核心转储”）。核心转储可用于进行根本原因分析和补救，并且可以保留在美国以便于进行工程设计工作。请注意，删除数据可能需要最多 60 天的时间，取决于具体的数据删除请求。

	路由日志： • 设备公共 IP 地址 • 组织 ID	最多 365 天（中国大陆地区）	故障排除和调试
	安全态势记录： • 请参阅表 1（不包括 IP 地址）	按需删除（中国大陆地区）	持续的功能使用情况和报告；故障排除
安全数据	安全 Web 网关		
	事件日志： • 源和目标 IP 地址 • 来源 ID • 组织 ID • 设备 ID • 时间戳 • 代理特定报头 • URL[2]	最多 31 天（中国大陆地区）	持续的功能使用情况和报告；故障排除
	防火墙即服务		
	管理服务日志（通常没有个人数据，但错误日志中可能会记录表 1 中的数据）	最多 30 天（中国大陆地区）	• 故障排除和调试
	事件日志： • 组织 ID • 来源 ID • 源和目标 IP 地址 应用 ID (公共/专用)	最多 31 天（中国大陆地区）	• 持续的功能使用情况和报告；故障排除
	防数据丢失 (DLP)		
	实时 DLP 事件日志： • 文件名/文件 ID • 触发违规的文本片段及周围文本（作为背景信息） • 在进行相关配置的情况下通过 AD/IdP 获取的用户身份数据	12 个月（中国大陆地区）	• 持续的功能使用情况和报告；故障排除 • 除非另有说明，否则不保留所检查的内容
	云应用发现		
	• 与用户或设备关联的云应用	90 天（中国大陆地区）	• 持续的功能使用情况和报告
控制平面数据（配置、策略、身份）	配置和策略数据		
	请参阅表 1	按需删除[6]（中国大陆地区）	• 持续的服务使用情况和报告；故障排除
	用户和设备身份数据		
	请参阅表 1	按需删除（中国大陆地区）	• 持续的功能使用情况和报告；故障排除
支持数据	请参阅表 1	按需删除（中国大陆地区）	• 确保在出现问题时提供有效的支持，并符合与向客户提供的服务的业务记录相关的神州云计算审计政策（即，合法商业目的）

对于 Cisco Security Cloud Control 数据保留和存储，请参阅上文第 3 节。

[6] 客户可以随时撤销 OAuth 密钥。

7. 个人数据安全

神州云计算已实施适当的技术和组织措施，旨在保护个人数据免遭意外丢失和未经授权的访问、使用、篡改和披露。

表 5

个人数据类别	个人数据类型	安全控制和措施 （受本表下方注释的约束）
账户数据	请参阅表 1	在传输和静态时加密
连接数据 （VPN 即服务、漫游）	请参阅表 1	在传输和静态时加密
设备安全态势数据	请参阅表 1	在传输和静态时加密
安全数据	请参阅表 1	在传输和静态时加密
控制平面数据 （配置、策略、身份）	请参阅表 1	在传输和静态时加密
支持数据	请参阅表 1	在传输和静态时加密

在传输时加密是指在通过互联网传输数据时，在 Secure Access China 数据中心之间对数据进行加密。如果客户使用 HTTPS 或其他加密通信方法（例如安全隧道），则在数据从用户传输至 Secure Access China 数据中心的传输过程中对数据进行加密。在同一数据中心内的 Secure Access 服务之间，某些数据可能以未加密的形式传输。除本节中所述的情况之外，Secure Access China 存储的所有数据（包括备份数据）均在静态时进行加密。

文件和其他流量内容在边缘数据中心以未加密的形式在存储器中进行处理，以完成检查并应用策略。身份数据在边缘数据中心使用随机生成的数字 ID 进行哈希处理。虽然客户可以选择某些 Secure Access China 套餐来配置其流量，以便此类流量不会在边缘数据中心被解密，但如果不进行这种解密，则只能根据 IP 地址和域元数据来确保安全性，并且客户将无法受益于 Secure Access China 的完整安全性功能。

对客户信息的访问受多重身份验证和授权机制的保护。通过一个账户管理应用程序来提供一个集中式接入点，以便跨多个平台提交账户请求并执行与此类请求相关的管理功能。所有资源都有一个负责人，负责确定将向谁授予对此类资源的访问权限。对资源的特权访问仅限于具有业务需求的授权用户，这与最小权限和基于角色和工作职能的职责分离的概念是一致的。

8. 受托处理个人数据的第三方

神州云计算与作为个人数据处理者受托方的服务提供商合作。个人信息处理的受托方可不时变更，本隐私数据表将进行更新以反映此类变更。

表 6

个人信息处理的受托方	个人数据	服务类型	数据中心位置
Atlassian (Jira)	支持数据	提供客户支持	中国大陆地区

AWS 中国	请参阅表 1	云基础设施提供商、事件日志数据仓库	中国大陆地区
思科	请参阅表 1 账户数据	协助神州云计算运营云服务。 Security Cloud Control (SCC)	中国大陆地区。将少数个人数据（例如，IP 地址）发送至美国，以便为服务补救、故障排除和支持提供协助。 为客户提供 SCC 服务。请参阅思科信任门户，查看 SCC 隐私数据表
Grafana 实验室	管理服务日志	监控基础设施和服务活动、汇总管理日志、进行服务故障排除和诊断	中国大陆地区
SendCloud	电子邮件信头数据 电子邮件正文	自动化的产品内置邮件，例如密码重置和账户开通邮件。	中国大陆地区

9. 行使数据主体权利

个人数据通过 Secure Access China 处理的用户，对通过此类服务处理的个人数据，有权请求访问、更正、暂停处理、数据迁移和/或删除，以及拒绝处理。

我们将在对此类请求做出回应之前确认您的身份。如果无法满足相关请求，我们会做出解释。请注意，如您是个人用户，我们可能会将请求转交给您的雇主单位以寻求响应。

如您要向神州云计算提出请求，可通过发送邮件至 ciscohosting@dcclouds.com 提交请求。 我们会尽力及时并以令您满意的方式回复询问和请求。