IoT/OT 安全与隐私-中国区

本文档的目的是向中国区购买或使用任何 IoT/OT 安全产品(企业 IoT 安全、企业 IoT 安全 Plus、医疗 IoT 安全或工业 OT 安全)的神州云计算客户提供所需的信息，以评估该服务对其整体隐私状况的影响，详细说明个人信息如何被该服务收集、处理、存储、使用等[1]。

1. 产品概要

由神州云计算在中国区运营的 Palo Alto Networks IoT/OT 安全订阅（以下简称“IoT/OT 安全”），利用物联网(IoT)、医疗联网设备(IOMT)和运营技术(OT)资产的各自特征和行为，为客户提供发现、分类和安全保护。通过分析网络上设备的行为，神州云计算运营的 IoT/OT 安全为企业提供准确的 IoT/OT 设备可见性和保护。

IoT/OT 安全有以下两个主要功能区。

IOT/OT 设备发现（Device Discovery)

该功能可识别和分类网络上的所有 IoT 和 OT 设备，为关键资产提供准确、实时的可视性和保护。这种无代理、被动式网络监控可确保脆弱的 IoT/OT 设备不会受到干扰。

IOT/OT 设备安全 (Device Security)

该功能可对正常设备行为进行基线分析，检测异常情况并生成警报。它可对整个组织进行实时风险评估，并为防火墙执行提供安全策略建议，帮助降低整体风险，确保业务连续性。IoT/OT 安全还会与防火墙共享检测到的 IoT/OT 设备身份，以便在安全策略中使用防火墙。在其 Device-ID 功能中将这些身份称为"IP 地址到设备映射"。

处理的信息

IoT/IOT 安全解决方案涉及处理网络数据的三个关键架构组件:

- **IoT/OT** (称为"产品")收集设备数据并将其发送到云中的安全服务。
- **日志服务**是一种基于云的服务，用于对产品发送的日志进行日志摄取、处理和可选存储(在 STRATA 日志服务中)，以供 IoT/OT 安全访问。

[1] 个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

- **IoT/OT 安全订阅在基于云的平台上运行，该平台使用机器学习、人工智能**和威胁情报来发现、分类和保护网络上的 IoT、医疗和 OT 设备。IoT/OT 安全应用程序处理来自日志服务的网络流量数据日志，并向产品提供安全策略建议和 IP 地址到设备映射，以用于安全策略(适用于产品)。用户通过 IoT/OT 安全门户访问动态丰富的 IoT/OT 设备清单、检测到的设备漏洞、安全警报和建议的策略集。

IoT/OT 安全订阅可访问产品的以下信息(适用于企业 IoT 安全；企业 IoT 安全 Plus；医疗 IoT 安全；工业 OT 安全)

通讯日志 (Traffic logs)-从设备和用户的 IP 地址获取内部和外部网络连接的信息。

威胁和 URL 过滤日志 (Threat and URL Filtering logs) -有关已知和未知威胁的信息，以及产品看到的网络流量。

HIP 匹配日志 (HIP Match logs)-登录 “GlobalProtect" 端点网络安全的端点信息。只有当连接的设备与配置的资产策略相匹配时，如主机未安装防病毒软件时，才会记录主机信息文件 (HIP) 数据。

配置日志 (Config logs)-有关对产品所做配置更改的信息，例如用户添加新安全规则时的信息。

系统日志 (System logs)-有关产品运行的信息，如许可证到期。

身份验证日志(Authentication logs) -有关最终用户尝试访问受身份验证策略规则控制的网络资源时发生的身份验证事件的信息。

GTP 日志 (GTP logs)-有关蜂窝设备通过蜂窝网络时的连接信息。一些蜂窝电话提供商使用 GPRS 隧道协议(GTP)数据为蜂窝电话设备创建安全策略。

隧道检查日志 (Tunnel inspection logs)-跟踪检查隧道会话开始和结束的条目。这些信息有时用于对隧道传输应用策略。

增强型应用日志 (Enhanced application logs)-执行分析所需的信息，如 MAC 地址、主机名、DNS 查询/响应和 Kerberos 验证信息。MAC 地址和主机名用于唯一识别网络上的设备及其模式，而 DNS 查询/响应则用于检测由高级恶意软件引起的出站通信。信息记录用户名，有助于识别未经授权的网络服务访问。

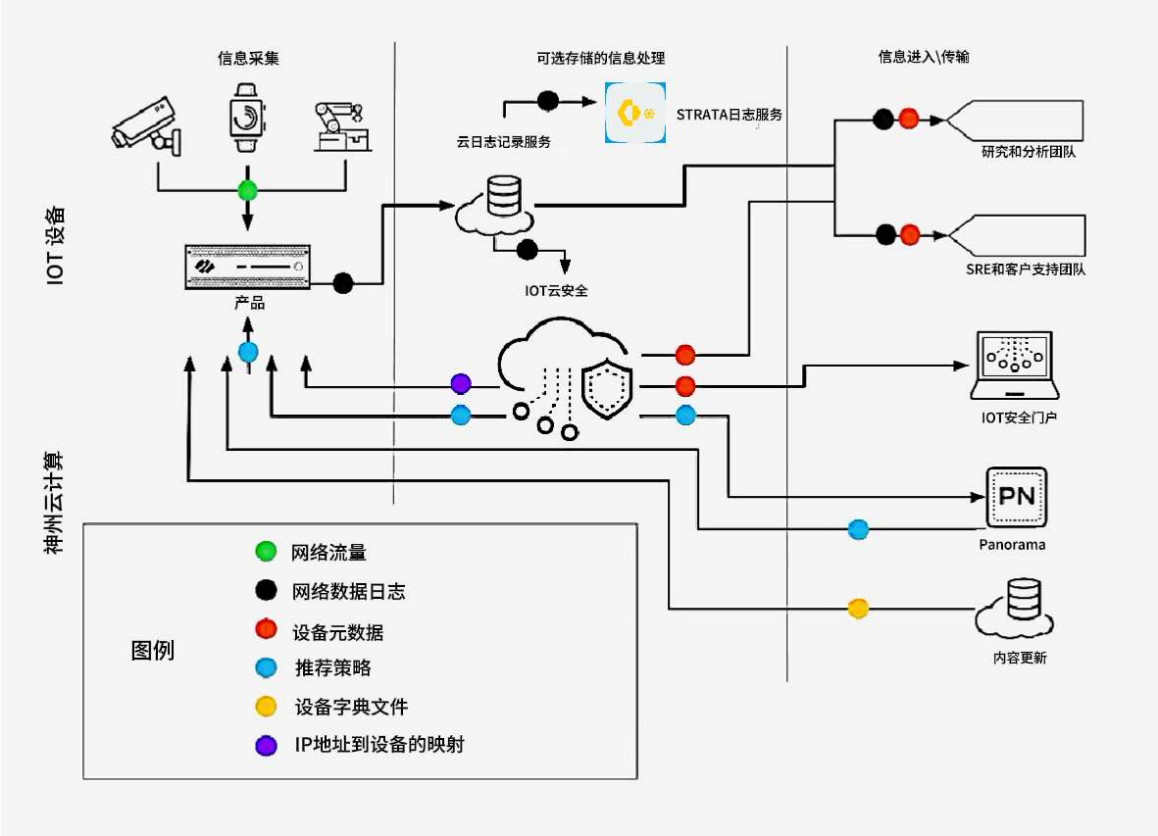
上述产品日志中的某些数据可能被视为或包含个人信息。下表详细列出了日志中包含的信息类别。

数据类别	发送到 IOT/OT 安全使用的日志服务的信息	可能包括个人信息
设备信息	MAC 地址	是
	主机名	是
	国际移动用户识别码(IMSI)	是
	国际移动设备识别码(IMEI)	是
	URL 或 DNS 请求中的限定主机名	是
	操作系统	没有
	防火墙名称	没有
	配置中使用的其他名称	没有
网络地址	源设备的 IP 地址	是
	目标设备的 IP 地址	是
其他信息	网址	是
	文件名	是

注:一般情况下，IoT/OT 安全订阅不会访问或处理上表所列产品日志数据以外的信息，这些数据可能被视为或包含个人信息。对于提供数据聚合和报告功能(例如，设备利用率洞察)的有限使用案例，网络传输中包含的个人信息数据(例如，与 IoT 设备传输的信息相关的患者姓名)将使用单向散列函数进行化名处理，在此类数据从产品日志发送到 IoT/OT 云之前，无法对个人信息进行解码。

数据流图

与本文件所述信息处理活动相关的主要 STRATA 日志服务如下所示。



数据处理的目的

IoT/OT 安全处理信息的目的是识别、分类和保护网络上的所有 IoT/IOMT/OT 设备，以提供准确、实时的视图并保护关键资产。

通过分析日志数据，IoT/OT 安全应用程序可生成以下类型的数据:

- 网络传输数据，包括设备网络传输量、设备网络目的地和设备应用程序/协议信息。
- 设备管理数据，用于设备资产管理、警报、用户配置、用户操作、IP 地址到设备映射、策略建议和报告。

受托处理者和处理地点

由神州云计算运营的 IoT/OT 安全中国区服务的数据托管在亚马逊云科技中国区域。神州云计算聘请了亚马逊云科技中国区域作为第三方服务提供商，该第三方服务提供商是神州云计算的受托处理者。

网络和设备监控的范围

防火墙管理员可以决定 IoT/OT 安全订阅将监控哪些网段，将这些网段的网络流量发送到云端。IoT/OT 安全只监控防火墙发送日志的网段中的设备。

我们的隐私保护措施

神州云计算根据 IoT/OT 安全与隐私-中国区采集、处理、存储和保护个人信息。

客户隐私选项

神州云计算的运营的产品旨在支持客户遵守中华人民共和国数据保护和合规义务。神州云计算通过在应用、网络和端点层面以及云中应对威胁情报和安全挑战实现。这些功能包括但不限于:数据本地化选项、策略执行、访问控制、日志记录功能。

访问和披露

客户访问

客户可通过 HTTPS IoT/OT 安全门户访问 IoT/IOT 安全应用程序处理的信息，该门户由神州云计算托管。IoT/OT 安全用户所有者可控制其用户对 IoT/OT 安全门户的访问。

管理员可以为 IoT 安全用户账户分配访问级别:所有者、管理员和只读。

神州云计算的访问

IoT/OT 安全门户网站的访问管理如下:

客户支持团队仅在客户管理员允许的情况下，可以访问客户 IoT/OT 安全帐户中存放在中国区域中的数据，在支持案例打开时用于故障排除。所有此类访问会被记录下来，客户可以查看。

跨境数据传输

如果在产品提供过程中，为更好的向用户提供服务，神州云计算可能需要与中华人民共和国境外的主体共享日志或信息，我们将按照适用的个人数据保护规定及数据出境等的合规要求进行，包括《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》等相关法律法规。

保留

IoT/OT 安全应用程序可保留一个月的网络传输数据(产品日志)、设备管理数据，如 MAC 地址、主机名、操作系统和网络地址(IP 地址、URL)，在亚马逊云科技中国区域最长保留一年，数据的保留均自数据产生之日起算。

客户可要求更改数据保留期，也可通过神州云计算客户支持要求清除用户数据。在用户停用

期间，用户数据将被清除。

安全

IoT/OT 安全解决方案基于多用户架构，将客户之间的数据分开。产品启动 HTTPS 连接到日志服务。该加密通道用于元数据传输。防火墙还通过 HTTPS 与 IoT/OT 安全应用程序通信，以获取 IP 地址到设备映射和策略建议。所有传输中和静止的数据都使用 TLS 和 AES-256 等加密技术进行保护。

神州云计算系统上存储或处理的任何数据均通过严格的技术和组织安全控制来保护。

第三方集成的安全性

IoT/OT 安全应用程序保存与第三方解决方案(如 Cisco ISE、ServiceNow 等)集成的凭证。凭证使用 AES-256 加密，然后存储在 IoT/OT 安全数据库的各个部分中，逻辑上按用户 ID 分开。采用严格的访问控制以确保只有特定的集成软件组件才能访问这些凭据。在凭证通过 HTTPS 安全地发送到相应的外部系统之前，通过 IoT/OT 安全后端服务器上的集成软件进行解密。解密凭证永远不会保存在 IoT/OT 安全系统的任何地方。

每个客户都有责任确保物理、技术和管理安全措施到位，以保护数据，并必须满足其组织要求的所有适用隐私和安全标准。

关于本 IoT/OT 安全与隐私-中国区

本文档提供的有关技术或专业主题的信息仅供一般认识之用，可能会有所变更，不构成法律或专业建议，也不保证适用于特定用途或符合适用法律。