科沃斯

产品安全白皮书

科沃斯机器人

全球领先的服务机器人创新者

版本号： 1.1

发布日期： 2026 年 5 月

摘要

在智能家居时代，数据安全与隐私保护已成为产品核心竞争力的重要组成部分。科沃斯机器人深知，信任是所有智能服务的基础。本白皮书旨在全面阐述科沃斯在产品全生命周期中融入的安全与隐私保护框架，详述我们在设备安全、通信加密、数据治理、云端防护及合规认证等方面的系统性实践。

我们遵循“安全-by-Design，隐私-by-Default”的原则，将国际标准的安全技术（如安全启动、端到端加密）与严格的内部管理流程相结合，并通过 ISO 27001、ISO 27701、ETSI EN 303 645、UL IoT Security 钻石级等多项权威认证持续验证我们的安全能力。科沃斯承诺，我们将持续投入，守护全球超过 3800 万家庭用户的每一次互动与每一份信任。

目录

DEEBOT X1 家族

智能清洁，安全护航

科沃斯公司简介

科沃斯机器人股份有限公司是一家全球领先的服务机器人公司，始终致力于通过创新技术提升人类的生活品质。自创立以来，科沃斯专注于智能家用机器人的研发与制造，成功推动了扫地机器人、擦窗机器人等产品进入全球数以千万计的家庭。目前，我们的产品与服务已覆盖全球超 3800 万家庭，并在欧洲、北美、亚太等主流市场建立了坚实的用户基础和品牌影响力。

通过构建开放的产品生态与技术架构，科沃斯为第三方开发者与合作伙伴提供了广阔的创新平台，共同推动智能机器人在家庭、商业及公共服务等多元场景下的应用深化。

我们的安全承诺与核心原则

随着产品智能化程度不断加深，科沃斯将**数据安全与隐私保护**视为产品设计的基石和我们对用户的核心承诺。我们坚信，唯有赢得用户信任，智能科技才能真正赋能美好生活。为此，我们将以下核心原则贯穿于产品与服务的每一个环节：

- **透明与可控：**我们以清晰易懂的方式告知用户数据的收集与使用目的，并提供直观的隐私控制选项，确保用户对自己数据的知情权和主导权。
- **安全-by-Design：**安全措施内置于产品设计之初，覆盖硬件、固件、应用、通信和云端全链路，采用符合国际标准的加密技术与安全协议。

- **数据最小化：**我们仅收集和处理实现产品功能所必需的数据，并通过匿名化、假名化等技术最大限度减少隐私风险。
- **端到端保护：**对用户数据实施从设备端到云端、从传输到存储的全程加密保护，严防未授权访问与泄露。
- **独立验证与持续改进：**我们定期接受权威第三方机构的安全审计与渗透测试，并通过国际认证验证我们的安全水平，建立持续改进的安全治理体系。

白皮书目标与范围

本白皮书旨在系统性地向用户、合作伙伴及公众展示科沃斯在产品安全与隐私保护领域的体系化建设成果。内容将涵盖**设备安全、应用安全、数据保护、通信安全、云平台架构**以及**合规认证**等关键领域。

通过本文件，我们希望您能清晰地了解科沃斯如何守护您的数据安全，并感受到我们致力于打造全球用户信赖的智能机器人产品的决心与能力。

科沃斯地宝 T80S

全方位技术安全措施

科沃斯构建了覆盖硬件、软件、通信与云端的“端-管-云”一体化纵深防御体系。本章将详细阐述在各层所实施的关键安全技术，确保产品在整个生命周期中的安全性与可靠性。

【图 1：科沃斯产品安全架构示意图】

硬件与固件安全

硬件与固件是产品安全的第一道防线。科沃斯从芯片选型与设计之初，即注入安全基因。

硬件安全启动链

科沃斯产品采用基于硬件信任根的安全启动机制。设备上电后，从 BootROM 开始，逐级验证下一阶段引导加载程序及系统内核的数字签名，确保只有经科沃斯官方签名的固件才能被加载执行，有效防止恶意软件或未经授权的固件在设备

上运行。

- 可信启动流程：Maskroom → SPL → UBOOT → KERNEL
- 防篡改保障：每一级固件均需通过上一级的密码学校验，形成完整的可信链。

【图 2：安全启动流程示意图】

调试接口安全管控

为保护核心知识产权并防止对设备的非授权访问，科沃斯对生产设备的调试接口（如 UART, JTAG）实施严格管控：

- 默认关闭：所有调试接口在出厂时均处于禁用状态。
- 授权访问：仅在售后维修等特定场景下，经由内部授权流程方可临时启用。
- 输出过滤：启用后的调试接口输出日志均经过敏感信息遮蔽处理，严防数据泄露。

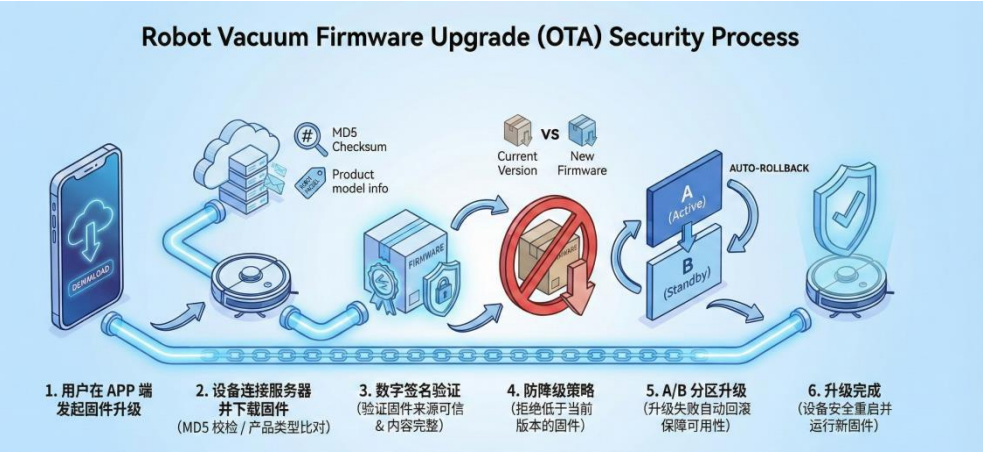
芯片级安全防护

- 读保护机制：主控芯片（MCU）启用读保护（RDP）功能，防止通过调试接口提取固件或敏感数据。

- 安全通信：在关键硬件通信链路（如 SPI/I²C）中，引入安全芯片或加密措施，保护总线数据传输的机密性，抵御硬件探针攻击。

固件更新与防降级机制

- 安全 OTA 更新：固件升级包均经过数字签名验证。设备在安装前会严格校验签名的合法性，确保更新来源可信且内容完整。
- 防降级策略：系统拒绝安装版本号低于当前版本的固件，防止攻击者利用旧版本已知漏洞进行破坏。
- 失败恢复（A/B 分区）：采用 A/B 双系统分区设计，当 OTA 升级过程中发生意外（如断电），设备可自动回滚至上一个正常工作的版本，保障设备可用性。



【图 3：安全更新流程示意图】

通信安全

科沃斯确保数据在任何网络通道中传输都受到强加密保护，防止数据在传输过程中被窃听或篡改。

设备与云端加密通信

- 强制 TLS 加密：设备与科沃斯云平台之间的所有通信均强制使用 TLS 1.2 及以上版本的安全加密套件进行传输加密和身份认证。
- 双向认证：设备与云端进行双向身份认证，确保设备连接至合法的科沃斯服务器，同时服务器也只对接入的合法设备提供服务。

本地网络接入安全

- Wi-Fi 安全：支持 WPA2/WPA3 等主流加密协议，保障设备接入家庭网络的安全。
- 受限的 AP 热点：设备在配网模式下开启的 AP 热点功能受到严格限制：
  - 仅开放必要的端口（如 8888）用于配网通信。
  - 热点具备超时自动关闭功能。
  - 严格网络隔离，防止通过设备 AP 热点攻击家庭局域网。
- 安全的蓝牙配对
  - 物理确认：关键绑定操作需通过设备物理按键确认，防止恶意绑定。
  - 链路加密：使用 BLE 4.2 及以上版本的链路层加密，保护配对过程。
  - 会话密钥：蓝牙控制指令通过每次会话动态协商的密钥进行加密，有效抵御重放攻击。

配网鉴权加密

设备配网过程采用基于证书的双向认证与非对称加密（如 x25519）协商对称密钥，最终通过高强度对称加密（如 AES-GCM）建立安全通道，从根本上杜

绝中间人攻击。

【图 4：安全配网流程示意图】

应用安全

客户端运行环境安全检测

科沃斯 App 具备运行环境安全检测能力，确保在可信环境中为用户服务：

- Root/越狱检测：通过多维度检查系统文件、属性、日志及行为特征，识别并警示运行在已 Root 或越狱设备上的风险。
- 模拟器检测：检测硬件特征、传感器参数及图形渲染性能，防止应用在模拟环境中被分析调试。
- 安全加固：应用代码经过混淆、加壳等安全加固处理，增加逆向工程难度。

本地数据加密与密钥管理

- 敏感数据保护：所有敏感用户数据（如地图、日志）在设备本地存储时均进行加密处理。
- 密钥安全：充分利用操作系统提供的安全存储区（如 Android Keystore, iOS

Keychain）管理加密密钥，确保密钥本身难以被提取。

用户账号与认证安全

- 强密码策略与多因素认证 (MFA)：鼓励用户设置强密码并提供 MFA 选项，为账户登录提供额外保护层。
- 会话管理：实施安全的会话令牌管理机制，包括空闲超时、令牌更新和防止会话固定攻击。
- 异常监控：对异常登录行为（如异地登录、多次失败尝试）进行实时监控和告警。

数据安全

- 文件在网络传输过程中，同时进行 SHA-256 的完整性校验，守护数据的“数字指纹”。
- 对于网络传输的数据进行格式、类型、长度等合法性校验，构建安全的第一道闸门。

视频安全

特定型号的家用机器人产品提供视频官方服务，包括安全警报和定点监控功能服务。

视频管家功能在用户调取机器人摄像头时，需进行二次密码验证，并通过加密传输与访问控制机制，确保家庭影像数据的安全与隐私不被越权访问。

【图 5：视频管家图示】

云平台安全

科沃斯云平台构建了具备纵深防御能力的安全体系，为 IoT 服务提供可靠保障。

云端基础设施安全防护

- 网络隔离与分段：严格隔离开发、测试与生产环境。在生产网络内部，根据不同工作负载的风险等级进行微分段隔离。
- DDoS 防护：部署分布式拒绝服务防护系统，保障服务可用性。
- 入侵检测/防御系统（IDS/IPS）：实时监控网络流量，检测并阻断恶意攻击行为。

身份认证与访问控制

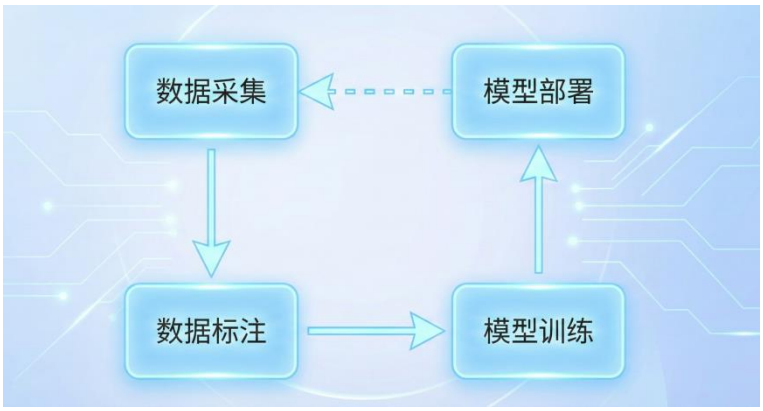
- 最小权限原则：遵循最小权限原则实施严格的访问控制策略（RBAC），所有 API 访问均需强制认证与授权。
- API 安全网关：所有服务 API 均通过统一网关发布，实施速率限制、防重放攻击等安全策略。
- 运维安全：所有生产环境运维操作均需通过堡垒机进行，并接受严格的审计日志监控。

安全监控与威胁检测

- 集中化日志审计：汇集所有关键日志进行集中监控与分析，实现安全事件的可追溯性。
- 威胁情报与异常检测：利用自动化安全监控工具实时检测潜在威胁和异常活动，并及时响应。

AI 算法训练和使用安全

- 训练阶段：合规采集核心数据，经匿名处理、清洗后构建数据集，用训练框架（如 TensorFlow）迭代训练模型，通过验证集调优；



【图 6：算法训练图示】

- 发布阶段：先多场景测试模型稳定性，再封装部署，搭配加密传输 / 隔离存储保障安全，上线后监控性能，按需更新优化。

DEEBOT *mini*

数据与隐私保护实践

科沃斯坚信，隐私是用户的基本权利。我们严格遵循全球隐私保护法规，并将“Data protection by design and by default”原则融入产品设计的每一个环节，确保用户对其数据拥有充分的透明度和控制权。

【图 7：数据和隐私保护图示】

隐私保护原则

【图 8：隐私保护原则图示】

我们的隐私实践基于以下核心原则：

- 合法、正当、透明： 我们仅在用户知情同意或其他法律允许的情况下处理数据，清晰告知数据收集的目的、范围和处理方式。
- 目的限制： 数据收集和处理仅用于实现明确的产品功能，绝不用于用户未同意的其他用途。
- 数据最小化： 我们仅收集实现功能所必需的最少数据。
- 存储限制： 我们严格按照法律法规的要求对数据进行存储。
- 完整性与保密性： 我们进行严格的访问控制，保障用户数据在传输和存储过程中的安全，防止未经授权的访问、泄露或破坏。
- 问责制： 我们建立完善的隐私数据治理流程和安全事件应急响应机制，承担隐私数据保护责任。

数据生命周期管理

【图 9：数据生命周期安全图示】

数据收集最小化

在数据收集环节，我们通过技术和管理手段践行最小化原则：

- 功能必需：仅收集房间尺寸、障碍物位置等必要的环境信息以提供清扫服务。
- 差分隐私技术：在需收集数据用于产品优化时，我们采用差分隐私等先进技术对数据进行匿名化处理，确保无法回溯到具体个人或家庭。
- 明确授权：任何新增的数据收集需求都会通过 App 提示重新向用户告知并在获取用户的明示同意或具备相应的合法基础前提下进行。

数据传输加密

所有离开设备的数据，包括地图、日志等，均在强加密通道（TLS）中进行传输，确保数据在抵达科沃斯安全云平台过程中的机密性和完整性。加密算法使

用国际推荐的算法、密钥强度和使用方式，具体如下表所示：

算法	使用秘钥强度	用法
AES	128 位和 256 位	加密
RSA	2048 位和 4096 位	签名，签名
ECC	256 位	签名
ECDSA	256 位	签名
Ed25519	256 位	签名

数据存储与匿名化处理

- 加密存储：所有用户敏感数据在云端均以加密形式存储，即使是系统管理员也无法直接访问明文内容。
- 分类分级：对数据实行分类分级管理，对不同安全级别的数据实施不同的访问控制和保护策略。
- 匿名化聚合：用于大数据分析的数据均经过聚合与匿名化处理，彻底去除个人标识符。

数据删除权

我们充分保障用户对其数据的权利：

- 数据删除：用户可通过 App 账户注销功能清除设备端和云端的个人数据。

用户权利保障

科沃斯产品提供了直观的隐私控制中心，用户可轻松：

- 管理用户数据授权设置：自主决定是否开启必要信息授权功能（如个人账号信息、移动设备信息等）。
- 产品改进计划：自主决定是否参与产品改进计划、产品推广服务等。
- 访问和更正数据：随时查看和修改智能生成的家庭地图模型。

【图 10：用户权利图示】

更多详细信息，请参阅科沃斯完整的隐私政策：

中国大陆地区：

https://gl-cn-wap.ecovacs.cn/content/agreementNewest/PRIVACY/DEFAULT/DEFAULT

新加坡：

https://gl-sg-wap.ecovacs.com/content/agreementNewest/PRIVACY/SG/DEFAULT

德国：

https://gl-us-wap.ecovacs.com/content/agreementNewest/PRIVACY/US/DEFAULT

美国：

https://gl-us-wap.ecovacs.com/content/agreementNewest/PRIVACY/US/DEFAULT

WINBOT W2S 全能基站版

安全审计与合规认证

科沃斯的安全与隐私保护能力不仅源于内部严格的管理，更通过了诸多国际权威第三方机构的检验与认证。这些认证是我们向用户兑现安全承诺的有力证明。

【图 11：安全审计与合规认证图示】

国际标准合规性

科沃斯的产品设计与运营流程全面遵循以下国际国内法规与标准：

- 国际隐私法规：《欧盟通用数据保护条例》（GDPR）、《英国产品安全与电信基础设施法案》（UK-PSTI）、《加州消费者隐私法案》（CCPA）等。
- 国际安全标准：ISO/IEC 27001（信息安全管理体系）、ISO/IEC 27701（隐私信息管理体系）、ISO/IEC 27018（公有云个人数据保护）等。
- 中国法律法规：《中华人民共和国网络安全法》《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》。
- 行业特定认证：积极符合 ETSI EN 303 645、EU RED-DA 指令等物联网产品专项安全标准。

产品安全认证

科沃斯多款主力产品已获得以下权威安全与隐私认证，标志着其安全水平达到了国际领先水平：

- ISO 27001 & ISO 27701 **认证：**科沃斯已建立并持续运营符合国际标准的信息安全及隐私信息管理体系，覆盖机器人研发、制造、APP 与云服务全流程。（认证机构：BSI，2021）
- ETSI EN 303 645 **认证：**科沃斯扫地机器人及割草机器人产品矩阵是全球首批通过欧洲物联网网络安全标准认证的产品之一，验证了其在抵御网络攻击、防止数据泄露方面的优异表现。（认证机构：TÜV Rheinland， 2021）
- UL IoT Security Rating **钻石级认证：**科沃斯 X8, X9, T80, X11 等系列产品获得 UL 物联网安全评级最高等级——钻石级（Level 5），表明其产品满足了全球最严格的消费类 IoT 安全标准要求。(认证机构:UL Solutions，2025)
- EU RED-DA **网络安全认证：**在欧盟 EN 18031 系列标准强制实施前，科沃斯产品已率先通过该认证，满足其 14 大类安全机制要求，具备在欧盟市场销售的网络安全准入资格。（认证机构：TÜV Rheinland & Intertek， 2025）
- TÜV Rheinland 2PfG CH0003 **隐私保护认证：**科沃斯 ECOVACS HOME App 及 IoT 云服务获得 TÜV 莱茵大中华区首张扫地机器人品类隐私保护认证，通过了 200 余项严格测试。（认证机构：TÜV Rheinland， 2024）
- UK PSTI COC **符合性声明：**科沃斯产品完全符合英国 PSTI 法案关于禁止默认密码、漏洞披露透明化及安全更新保障的核心要求，已在官网公示合规声明。（认证机构：TÜV Rheinland， 2024）

- **CQC 物联网安全与个人信息保护认证：**科沃斯产品通过中国质量认证中心的权威测评，符合 CQC1167-2023 和 GB/T 40979-2021 标准，满足中国市场监管要求。（认证机构：CQC， 2023）
- **AU-ACT COC 认证：**2025 年 3 月 5 日，澳大利亚政府正式发布《网络安全（智能设备安全标准）规则 2025》，作为《网络安全法 2024》核心细则，该规则将于 2026 年 3 月 4 日生效，旨在应对智能设备网络安全挑战。我们地宝 X11 取得 TUV 莱茵该法规的第一张符合性证书。（认证机构：TÜV Rheinland， 2025）

渗透测试与第三方审计

我们坚信“信任，但需验证”。因此，我们定期聘请全球顶尖的网络安全公司对我们的产品、App 和云平台进行渗透测试和红队演练。在 2025 年度，我们邀请了奇安信和南德对产品、APP、云平台和在线商城进行了渗透测试，主动发现并修复漏洞。同时，我们每年接受第三方审计机构对我们的信息安全和隐私管理体系进行监督审核，确保持续符合 ISO 等标准的要求。

A CUT ABOVE THE REST

GOAT G1

1600m²

ECOVACS GOAT G1

应急响应与未来承诺

安全防护是一个动态演进的过程。科沃斯不仅致力于构建强大的事前防御体系，也建立了高效的事后响应机制，并承诺对安全进行持续投入。

漏洞管理流程

我们高度重视来自外部的安全反馈，并建立了公开、透明、高效的漏洞收集与响应机制。

- 官方漏洞披露渠道：我们运营网络安全应急响应中心（PSIRT）和安全邮箱，欢迎安全研究人员、用户及合作伙伴向我们报告潜在的安全漏洞。
- 标准化处理流程：我们对收到的每个漏洞报告都会遵循接收－评估－修复－发布－披露的标准流程进行处理，并与报告者保持密切、专业的沟通。
- 漏洞奖励计划：我们计划推出漏洞奖励计划，以感谢和奖励那些为科沃斯产品安全做出贡献的研究人员。

安全事件响应机制

为有效应对潜在的安全事件，我们制定了详尽的安全事件应急响应预案。

- 快速响应：我们致力于在发现安全事件后 72 小时内启动应急响应，并依法依规向监管机构和受影响的用户进行告知。
- 根因分析：任何安全事件都会进行彻底的根因分析（RCA），并据此改进我们的产品、流程和体系，防止同类事件再次发生。
- 持续监控：7×24 小时的安全监控体系确保我们能够及时发现异常

并采取行动。

持续改进与未来规划

安全没有终点。科沃斯承诺将安全与隐私保护作为长期核心战略，持续投入：

- 技术前瞻性研究：我们将持续跟踪前沿安全技术（如 HSM 硬件密码方案、AI 安全），并适时将其融入产品规划，以应对未来威胁。
- 合规体系拓展：我们将积极应对全球不断出台的新法规、新标准，确保产品持续满足各国市场的准入要求。
- 生态与供应链安全：我们将安全要求延伸至供应链与合作伙伴，共同提升整个生态系统的安全水位。
- 用户安全教育：我们将通过多种渠道持续与用户沟通安全最佳实践，共同守护智能家居环境的安全。

科沃斯承诺，为用户提供不低于 3 年的固件安全更新支持，确保产品在整个生命周期内都能获得最新的安全保护。

科沃斯清洁机器人DEEBOT PRO

全场景 全能 商用清洁方案

共建可信智能未来

在科沃斯，我们深信，真正的智能始于信任。每一台走入家庭的机器人，承载的不仅是清洁家居的责任，更是用户对我们守护其数据安全与生活隐私的嘱托。

本白皮书系统阐述了科沃斯在产品安全与隐私保护领域的体系化思考、技术实践与合规成就。从硬件安全启动到云端加密存储，从数据最小化原则到国际权威认证，我们构建了多层次、纵深化、全生命周期的防护体系。这一切的背后，是科沃斯“**以用户为中心，安全**-by-Design”的核心理念。

然而，我们深知，安全之路，道阻且长。我们将始终保持敬畏之心，以透明、开放的态度，与用户、安全社区、行业伙伴及监管机构紧密合作，共同应对未来的安全挑战。

我们承诺，科沃斯将一如既往地将资源投入到安全与隐私保护中，不断夯实我们的技术、流程和管理体系。我们的目标不仅是制造卓越的清洁机器人，更是成为全球用户最值得信赖的智能科技伙伴。

让我们携手，共同打造一个更清洁、更智能、更安全的未来。


科沃斯机器人
致力于创新科技，守护每家信赖
了解更多：www.ecovacs.com