OriginOS

安全白皮书

vivo 出品 2021.12

OriginOS

OriginOS

01 概述

信息安全和隐私保护是一个企业获得消费者信任和依赖的基石，是每位消费者的基本权利，vivo 作为一家科技企业，有义务和责任保护每位用户的数据不被泄露，隐私不被侵犯，使用手机的过程不被窥探和跟踪。为此，vivo 制定了最严苛的隐私保护体系与安全合规原则，在产品开发设计、销售和使用的每一个环节中，严格遵循全球各国安全合规要求，从用户使用手机的场景和痛点出发，通过科技创新，守护好每一位用户的信息与隐私安全。

无论是社会，还是企业，甚至是个人，对数据的依赖越来越强，导致了数据安全和隐私保护面临的挑战也越来越大。如何更好地保护用户的隐私，成为了安全与隐私工作的重中之重。为此，vivo 经过对行业的深入洞察分析和内部实践经验总结，明确了隐私保护的三大原则：

1. 透明可控，设备上各应用服务的隐私数据的使用情况可查看、可管控；
2. 隐私端侧处理，隐私数据在不出设备的前提下为用户提供定制化的各类服务；
3. 数据最小化，使用特别是分享数据时，严格对非必要的隐私数据进行过滤。

隐私保护三原则已经融入到 vivo 产品和服务的设计、实现、运营的全过程中，在数据流动的全链路、用户体验的全场景中，进而能全面守护用户隐私。

基于 vivo 的隐私保护三原则构建了 OriginOS 安全体系，如图 1 所示。

图 1：OriginOS 安全体系

OriginOS

OriginOS 安全体系中的主要模块简述如下：

1 硬件安全

为 OriginOS 提供信任根和硬件的安全保护，包括安全启动、硬件加解密引擎、设备唯一密钥、设备证明、安全元件、安全存储等。

2 系统安全

为 OriginOS 及内核提供了安全保护，包括系统完整性保护、系统安全更新和防回滚、SELinux 强制访问控制、漏洞防御、基于生物特征的身份认证、可信执行环境以及网络与通信安全等。

3 应用安全

为移动应用提供了通用的基础安全能力，包括应用上架安全监测、应用签名验证、应用运行保护、基于 AI 的应用行为监测、仿冒应用检测、防诈骗防骚扰等。

4 高安全级别应用保护

为涉及用户机密信息、敏感信息的应用提供了高安全级别的保护，包括支付保护功能、信息验证码保护功能、安全键盘等高级别的安全能力，以及基于安全元件保护的高级别安全应用，如 vivo Pay、手机交通卡、eID 安全身份认证、手机车钥匙等。

5 云服务与设备管理安全

为用户的云服务及设备管理提供安全保护，包括 vivo 帐号数据安全、vivo 帐号风控措施、vivo 设备管理等。

6 数据安全

为数据的传输、存储和使用提供了安全保护，包括密钥管理、云服务数据备份、文件级加密、密码保险箱、TF 卡数据加密、数据删除等。

7 隐私保护

为用户的敏感信息提供了保护，包括权限管理、定位隐私保护、录音录像隐私保护、隐私密码、原子隐私系统、差分隐私等。

除了使用科技创新守护用户隐私，我们认为，隐私保护的功能还需要更透明可控的安全设计、更优雅易用的安全体验、更关注特殊人群的隐私保护需求 ..... 总之，应该以更人文、更有温度的科技，守护用户隐私安全，这也践行于我们安全产品设计的始终。

02 硬件安全

OriginOS 基于软硬件一体的安全解决方案来提供安全性，通过安全启动、可信执行环境、安全存储等特性来确保从系统启动到应用程序的运行均有安全验证机制，并且最大程度保证上层应用、数据的安全。

2.1 安全启动

安全启动是设备启动过程中，对每个启动阶段所包含的组件在加载运行之前都须经过验证，以确保所加载组件的完整性、合法性，它是以固化在 SoC（System on Chip，片上系统）片内的引导程序（ROM SoC Bootloader）作为安全启动的硬件信任根；只有成功通过完整性校验，才能继续下一步的组件加载运行。如此，通过反复地校验、加载运行下一个组件，从而形成安全启动链。安全启动过程中的组件包括引导加载程序、内核、内核扩展项和基带固件等。安全启动链能确保底层系统软件的合法性、完整性和真实性，从而确保移动设备正确、安全、可靠地运行 OriginOS。

2.2 硬件加解密引擎

在移动设备上，安全、速度、节能都至关重要，OriginOS 同时满足了设备对于这三者的要求。硬件加密引擎支持的主要算法有：

1. 3DES
2. AES-128、AES-256
3. SHA-1、SHA-256
4. HMAC-SHA1、HMAC-SHA256

* 注：部分机型未搭载硬件加密引擎。

2.3 设备唯一密钥

设备唯一密钥（HUK，Hardware Unique Key）是特定于每一个设备的密钥，能唯一标识设备且无法被篡改，仅有硬件加密引擎可以访问。HUK 固化在芯片内，主要用于派生出其他密钥，例如，用于锁屏密码保护的密钥、文件系统加密的密钥、指纹模版保护的密钥等。

2.4 设备证明

为了确保 OriginOS 设备是真实可信的，vivo 在产线就预置了设备证书以及相应的公私钥对，用于标识设备的合法身份。设备私钥在 TEE（Trusted Execution Environment，可信执行环境）内部生成且被加密保存在 TEE 内部，TEE 外部无法访问。在某些对安全性要求较高的应用场景中，应用可以向 vivo 服务器发起验证，以确定该设备的真实性。

* 注：部分机型未预置设备证书。

2.5 安全元件

安全元件（Secure Element）是一种用于存储敏感数据并能运行安全应用程序、以及抵御外部恶意解析等攻击的专用芯片。在 OriginOS 设备上，安全元件用于存储密钥等敏感数据，以提升移动支付等业务的安全性。安全元件通过了 CC EAL6+（硬件）、EAL5+（软件）安全认证，以及 EMVCo 等国际标准认证，符合金融行业移动支付标准的要求。

* 注：此功能仅在部分机型的产品上提供。

2.6 安全存储

OriginOS 能基于安全文件系统（SFS）为 TEE 提供安全的存储服务，能为 TEE 存储敏感数据，如密钥、证书、个人隐私数据和指纹模板等。

TEE 中运行的 TA（Trusted Application，可信应用）可通过安全存储 API 接口对敏感数据进行加密，并存放于安全文件系统中，加密后的敏感数据只有该 TA 本身能够访问，其他 TA 及外部应用无法访问。

安全存储所使用的加解密密钥在 TEE 内部基于设备 HUK 进行派生获得，且敏感数据加解密的过程也在 TEE 内部执行，因此，该密钥生成后不会流出设备 TEE 安全区，可信应用之外的其他应用无法读取该加解密密钥。

基于重放保护内存（RPMB，Replay Protected Memory Block），OriginOS 还提供了保护用户机密数据和系统数据的能力，以及防止非法删除和访问这些受保护的数据。RPMB 由 TEE 直接进行安全管理，只有 TEE 能根据相应的安全协议（即命令操作码和数据结构）访问 RPMB。该安全协议基于计数器、HUK 派生的密钥和 HMAC（哈希消息认证码），对 RPMB 的读 / 写进行签名和验签，从而防止重放攻击，确保数据不被恶意覆写或篡改。可信应用之外的其他应用无法访问 RPMB 提供的访问接口。

03 系统安全

系统安全的目标是基于硬件芯片安全构建系统层基础安全能力，包括有系统完整性保护、系统安全更新和防回滚、SELinux、漏洞防御、可信执行环境、网络与通信安全等。

3.1 系统运行安全

3.1.1 系统完整性保护

验证启动（Android Verified Boot）设计了一个需要硬件支持才能正确实施系统软件完整性验证的框架。OriginOS 的验证启动是使用签名公钥，来验证程序或系统镜像的签名是否真实有效，以确保移动设备启动之后所加载的引导程序是来自 vivo，然后通过建立一条从受硬件保护的信任根到引导加载程序、再到 boot 分区和其他分区（如 system 分区、vendor 分区）的完整信任链，使得设备启动过程中，无论是在哪个阶段，都会在进入下一个阶段之前先验证下一个阶段系统镜像的完整性，确保其未被恶意篡改。

3.1.2 系统安全更新和防回滚

OriginOS 提供了 Android 原生的 OTA（Over The Air，空中下载）机制，以方便用户下载和安装较新版本的系统软件及增强的安全功能，从而及时修复系统可能存在的安全漏洞。当触发 OTA 更新时，系统首先对 OTA 下载的升级包进行完整性校验；校验成功通过后，重启系统进入系统恢复模式，再进行升级包的签名校验，同时匹配升级包的版本以及安全补丁日期等信息，防止系统软件更新到存在漏洞的低版本；最后设备再将升级包中的内容写入系统存储。

OriginOS 还支持基于硬件的防回滚(Anti-Rollback)机制，每台设备的主芯片内部 Fuse 空间中会烧写防回滚值，同时在软件镜像中也会记录防回滚值。在开机启动阶段对该值进行判断，能确保设备上只允许安装较新版本的系统软件，以防止设备上的系统软件降级到存在安全漏洞的低版本。

3.1.3 SELinux 强制访问控制

SELinux 为 Android 系统提供了一个灵活的、可配置的 MAC（Mandatory Access Control,强制访问控制）机制，通过为系统中每个实体（如进程、应用、文件等）设置访问权限，实施访问控制，从而为系统提供安全保护。

OriginOS 借助 SELinux 能减少或防止系统遭受 root 攻击。非法应用 / 恶意软件可以利用系统或内核的潜在漏洞，获得原本不具有的 root 访问权限，实现 root 攻击，从而完全控制用户移动设备。OriginOS 基于 SELinux 强制访问控制（MAC,Mandatory Access Control）使得非法应用 / 恶意软件无权访问系统或内核的潜在漏洞；同时 OriginOS 还对来自应用程序的攻击进行检测和拦截，从而减少或阻止系统遭受 root 攻击。

OriginOS 借助 SELinux 能保护用户的敏感数据。非法应用 / 恶意软件可以利用合法应用程序的缺陷，访问或修改未经允许的用户敏感数据。OriginOS 基于 SELinux 通过标识应用程序、设置访问权限并严格执行访问控制，使得非法应用 / 恶意软件无权访问用户敏感数据，实现对用户敏感数据的安全保护。

OriginOS 借助 SELinux，还可以保护和限制系统服务、控制对系统日志的访问、降低非法应用程序 / 恶意软件对系统安全带来的影响，并保护用户免遭移动设备上的代码可能存在的缺陷或潜在漏洞的影响。

3.1.4 漏洞防御

（1）内核地址空间布局随机化（KASLR）

Android 用户地址空间的加固使得底层 Linux 内核成为攻击者更具吸引力的目标。OriginOS 引入了内核地址空间布局随机化（KASLR），每次内核启动时，获取一个随机生成的内核镜像偏移值，让内核镜像的映射地址相对于链接地址有个随机的偏移，从而能随机化内核代码加载的位置，进而帮助缓解内核漏洞。

（2）特权模式访问禁止（PAN）/ 特权模式执行禁止（PXN）

OriginOS 支持 ARM 的特权模式访问禁止（PAN）/ 特权模式执行禁止（PXN），实现内核模式和用户空间的隔离，从而禁止内核模式访问用户空间数据和禁止内核模式执行用户空间代码。

由于编程错误或系统遭受攻击，操作系统可能会访问用户空间的数据，从而带来用户敏感数据泄漏的风险。基于特权模式访问禁止（PAN），能在此类访问发生之前捕获这种非特权数据的意外访问，从而确保用户空间数据的安全访问，防止用户敏感信息泄露。

攻击者可能通过篡改内核页表指针从而在用户空间执行用户代码，实现攻击目的。为了缓解这种漏洞，基于特权模式执行禁止（PXN），通过在内核模式下将用户空间页标记为不可执行，从而防止当处理器在内核状态下试图执行用户空间代码。

3.1.5 基于生物特征的身份认证

生物识别是一种利用人体生物特征进行身份认证的技术，旨在使得用户在确保安全的前提下获得更加便捷的身份验证体验。OriginOS 主要提供了指纹识别和面部识别两种生物识别方式。

（1）指纹识别

OriginOS 支持多种指纹识别方案，包括后置指纹、侧边指纹、屏下单点指纹和屏下大面积指纹等，具体的技术实现包括电容、光学、超声波等。

OriginOS 指纹识别架构如图 2 所示。

OriginOS 指纹识别采用 TEE 安全隔离机制，将数据采集、数据传输、特征比对、防伪检测等过程运行于 TEE 安全环境中。用户录入的指纹数据会经过 TEE 安全环境被不可逆地处理成不可识别的数字信息，然后加密存储在手机的安全文件系统中，密钥由 HUK 派生而来，确保数据仅能在本机 TEE 安全环境中使用。

OriginOS 指纹识别可以应用于手机锁屏解锁、隐私与应用加密、第三方应用登录认证、支付认证等场景，外部应用只能获取到最终的识别结果。OriginOS 不会将指纹特征信息发送给任何第三方，采集的过程数据会在识别结束后立即销毁，即便手机被 root 也无法获取到用户的任何生物数据信息。

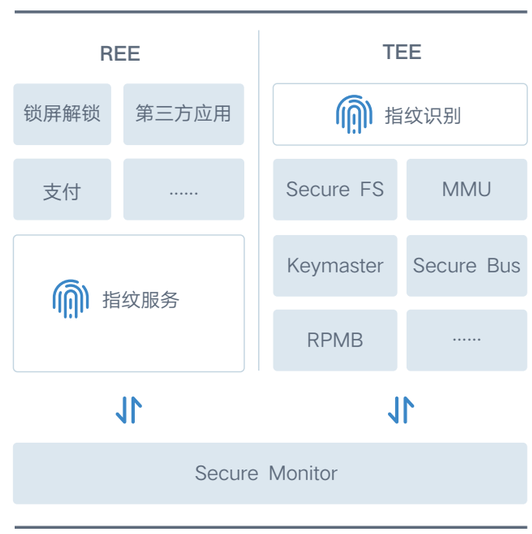

图 2：OriginOS 指纹识别架构

OriginOS 指纹识别支持防暴力破解机制，当指纹识别连续失败 5 次或者重启开机之后都将会禁用指纹识别功能，需要手动输入密码才能激活。当用户 72 小时内未使用过密码解锁时，则需要输入密码来激活指纹识别功能。这样不仅能加强手机的安全性，同时还能加强用户对密码的记忆，防止长时间未输入密码导致将密码遗忘。

指纹识别的错误识别概率极低，概率大约为五万分之一。为满足用户更高的安全需求，OriginOS 指纹识别是基于屏下大面积指纹提供的双指认证方案，错误识别的概率将大大降低至二十五亿分之一。

如果用户担心指纹错误识别的情况，建议使用密码来进行身份验证。

（2）面部识别

OriginOS 面部识别通过前置摄像头获取面部信息，基于神经网络算法对面部信息进行身份认证。

OriginOS 面部识别架构如图 3 所示。

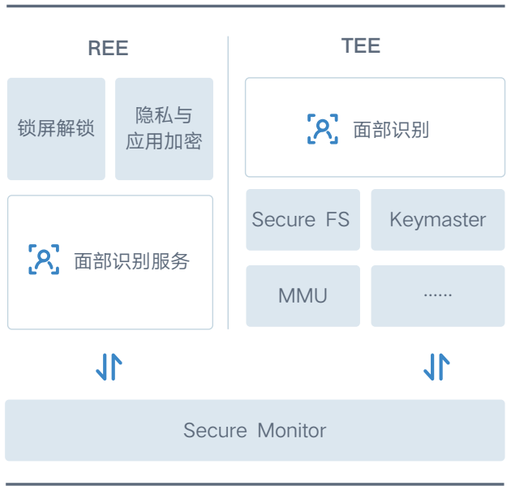

图 3：OriginOS 面部识别架构

用户录入的面部特征数据会经过 TEE 安全环境被不可逆地处理成不可识别的数字信息，然后加密存储在手机的安全文件系统中，密钥由 HUK 派生而来，确保数据仅能在本机 TEE 安全环境中使用。面部信息对比过程也完全运行在 TEE 安全环境中，外部应用只能获取到最终的识别结果。OriginOS 不会将面部特征数据发送给任何第三方，基于前置摄像头采集的图片在与存储的面部特征完成特征匹配对比之后就会立即销毁，不会将识别图片进行保存，即便手机被 root 也无法获取到用户的任何生物数据信息。

OriginOS 面部识别支持防暴力破解机制，当面部识别连续失败 5 次或者重启开机之后都将会禁用面部识别功能，需要手动输入密码才能激活。

当 72 小时内未使用过密码解锁时，需要输入密码来激活面部识别功能。这样不仅能加强手机的安全性，同时还能加强用户对密码的记忆，防止长时间未输入密码导致将密码遗忘。

面部识别的错误识别率极低，概率大约为五万分之一。对于长相相似的双胞胎、亲属以及未满 13 岁的儿童，错误识别的概率会增大。若用户担心面部错误识别的情况，建议使用密码来进行身份验证。

3.2 可信执行环境

OriginOS 基于 ARM TrustZone 技术为移动设备提供 TEE (Trusted Execution Environment，可信执行环境），如图 4 所示。基于隔离的安全原则，TEE 为应用提供硬件级别的安全保护。

ARM TrustZone 技术将 CPU（Central Processing Unit，中央处理器）分为了非安全世界（Normal World Status，NWS）的工作态和安全世界（Secure World Status，SWS）的工作态。

通常称非安全世界运行的环境为富执行环境（Rich Execution Environment，REE），主要负责处理对功能性、开放性等要求较高的业务；称安全世界运行的环境为可信执行环境（Trusted Execution Environment，TEE），主要负责处理对安全性、私密性要求较高的业务。

TEE 提供了密钥管理、加解密、安全存储等服务，为密钥安全存储、移动支付、指纹识别、人脸识别等设备上最核心的敏感数据提供了高等级的安全与隐私保护。

图 4：可信执行环境的框架

3.2.1 安全存储

TEE 的安全存储功能为用户提供安全存储机制，保证数据的机密性和完整性。安全存储支持设备绑定，还支持不同可信应用之间的隔离。

可信应用通过调用 TEE 中安全存储的 API 接口，对敏感数据进行加解密，然后进行安全存储和访问。每个可信应用仅能访问自己存储的数据，而无法访问、删除或篡改其它可信应用存储的数据。

TEE 的安全存储分为两种：安全文件系统存储与 RPMB 存储，前者将密文存储到特定的安全存储分区，后者将数据存储到 Flash 特定的存储区域，RPMB 支持防删除、防重放攻击等功能。

3.2.2 加解密服务

TEE 支持多种对称密钥算法、非对称密钥算法以及哈希算法，如 AES、RSA、ECDSA、SHA 等，为第三方开发的可信应用提供加解密、数字签名、签名验证、数字摘要等服务。TEE 提供的加解密服务遵从 GP TEE 标准。

密钥将存储在安全元件或严格加密的安全存储空间中，从而保证密钥的安全性。用户可根据业务的需要，开发可信应用来使用加解密服务。

3.2.3 可信用户交互

在非安全世界 REE 侧的应用环境中，用户需要输入很多机密信息，如登录密码、PIN 码、信用卡帐号、支付密码等，才能访问各种业务。然而，这些机密信息会因为系统漏洞或外部攻击而被窃取。

可信用户交互（TUI）基于启动、停止、触摸检测等底层 API，在用户和可信应用之间直接建立安全通道，让可信应用能通过通用的显示器、触摸屏直接与用户进行安全交互，即让用户将敏感数据直接输入到可信应用，同时还能抵御按键记录、屏幕获取、机密信息的篡改或遮掩、钓鱼等攻击。通过 TUI 建立用户和可信应用之间的安全通道，实现与非安全世界 REE 完全隔离，从而能完全阻止在用户输入机密信息时 REE 侧对显示区域和触摸屏的访问。

3.3 网络与通信安全

3.3.1 WLAN 安全检测

用户在连接 WLAN 网络尤其是公共环境的 WLAN 网络时，可能会存在隐私被窃取的安全风险，如窃取用户的帐号密码等。OriginOS 会对当前用户设备所连接的 WLAN 网络进行动态的安全检测，检测项包括：ARP 攻击检测、中间人攻击检测、DNS 服务器劫持检测等。若 OriginOS 检测到 WLAN 网络风险，会及时告知用户来保障用户隐私。

同时为了提高风险识别的准确性和精确性，OriginOS 基于大数据和机器学习，根据用户不同的网络连接场景，动态地调整触发频率和检测阈值，从而最大程度地保证用户在公共场所下连接 WLAN 网络的安全性。

3.3.2 伪基站的检测和防护

攻击者会通过伪基站来获取用户的身份信息、发送广告及诈骗短信，甚至拦截用户的短信验证码，严重威胁用户财产及信息安全。OriginOS 通过对 GSM/LTE 伪基站系统消息的特征字段提取、识别和打分，来确认伪基站的风险等级，然后根据伪基站的风险等级，使用不同的限制策略，以限制终端接入伪基站。

* 注：LTE 伪基站识别仅部分平台支持。

OriginOS

04 应用安全

vivo 为应用提供了全过程全链路的安全解决方案：

1 应用上架阶段，对应用进行严格的安全检测，同时为开发者提供便捷的安全检测服务，尽早约束不合规行为，确保上架应用的安全；

2 应用安装阶段，对应用进行签名校验、病毒木马扫描、仿冒盗版鉴定等，确保所安装应用的安全；

3 应用运行阶段，通过应用沙箱、运行时内存保护、安全输入等机制确保应用本身数据的安全性；

4 确保应用运行环境的安全，在 OriginOS 系统层面提供了静态威胁检测、基于 AI 的应用威胁检测、恶意网址检测等机制，最大程度保障用户使用应用的安全性。

4.1 应用上架安全检测

vivo 借助静态检测、动态监测、场景检测等技术，确保应用上架前的安全性；借助隐私政策检测、敏感权限检测、数据采集和使用检测等技术，确保应用上架前的合法性。

vivo 开发者平台还支持为开发者提供国家法律法规条款的解读，帮助开发者识别出应用中存在的不合规的安全风险，以及根据相关的条款对不合规的应用提供整改的指导建议，以规避这些安全风险，从而提高上架应用的质量。

4.2 应用签名验证

OriginOS 要求所有应用必须先使用证书进行数字签名，然后才能安装到设备上或进行更新。

开发者通过应用签名，可以标识其应用并更新其应用，可以将 vivo 和开发者的信任关联起来，可以让开发者知道其应用以未经篡改的方式安装到设备，还可以对其应用的行为进行负责。

OriginOS 通过应用签名，在安装应用时，确保所安装应用未被篡改；在运行应用时，确保不同的应用签名将分配不同的用户 ID，进而放入不同的沙箱进行隔离，确保每一个应用无法访问其他应用的数据；在应用升级时，确保只有相同的应用签名，才可以进行应用更新，防止恶意应用通过更新的方式替换现有应用。

4.3 应用运行保护

应用在安装时，OriginOS 会给应用分配一个指定的存储目录，该指定存储目录仅允许该应用访问，其他应用无法访问，从而确保应用的静态数据安全。

在启动应用运行时，OriginOS 根据应用签名，为应用分配一个独一无二的用户 ID (UID)；然后根据该 UID 设置一个内核级应用沙盒，让该应用在该沙盒中运行。应用在运行过程中，OriginOS 会对应用采取强制访问控制（MAC，Mandatory Access Control）等措施，防止应用执行越权访问，以确保应用运行时的安全。默认情况下，应用之间不能进行交互，且对操作系统的访问权限也会受到限制。

4.4 应用安全检测

i 管家提供的安全检测功能可防止病毒木马、恶意应用、仿冒应用、诈骗应用对手机的侵害，以保护用户的个人隐私和财产安全。

i 管家的安全检测集成了多引擎扫描策略，在应用安装与主

动检测时自动进行多维度全方位的安全性检测，提升扫描能力及效率，保证用户在联网、弱网、无网络等各种环境下的安全扫描流畅进行。

同时提供了风险应用隔离箱功能，能使放入隔离箱内的应用行为受到一定限制，进行安全风险隔离，即使运行存在安全风险的应用，系统也能免受风险威胁。

4.5 仿冒应用检测

仿冒应用，是仿造知名应用的非官方应用。仿冒应用不仅损害了开发者的利益，而且会导致用户隐私泄露和财产损失的风险。OriginOS 对应用的生命周期进行全方位防护，在应用安装前及 i 管家进行安全检测扫描时，将应用的身份信息特征与正版应用库特征进行对比，识别该应用是否是仿冒的，从而降低安全风险。

4.6 基于 AI 的应用行为监测

面对恶意应用的快速变种，传统引擎无法及时识别出来。OriginOS 将应用行为监测与传统引擎进行结合，通过在系统中埋入行为桩点信息，将应用程序触发桩点的行为序列输入到本地 AI 模型，来对应用行为做出智能分析和判断，从而确定应用是否存在风险，并配合传统安全引擎，有效降低快速变种的恶意应用所带来的安全风险，做到低功耗、高智能的实时终端安全防护。

4.7 防诈骗防骚扰

OriginOS 预置的 i 管家“防骗中心”功能可进行诈骗电话拦截、诈骗短信拦截、恶意应用检测、诈骗风险鉴定等，以帮助用户减少或免遭诈骗风险。

1 骚扰电话拦截

为用户拦截骚扰电话。用户可通过个性化定制标记号码、黑名单、开头号码、归属地、海外号码等多种拦截规则，有效拦截推销、诈骗等骚扰电话，净化个人通话环境。

2 骚扰信息拦截

为用户拦截骚扰信息、垃圾信息等。用户可通过设置智能云拦截策略、本地拦截策略、号码黑名单、关键词黑名单等方式对不良信息进行有效拦截，以帮助用户免受骚扰信息的困扰。

3 恶意网址检测

OriginOS 提供恶意网址检测服务。通过对用户所访问的网站进行安全性检测，识别恶意网站并提醒用户。目前支持的检测种类有：钓鱼类（如伪造银行、运营商、电子商务等各种非正规网站）、下载类（如系统破坏、木马等）、非法类（如博彩、色情等）、病毒类（如代码命令、远程控制等）等。

OriginOS

05 高安全级别应用保护

本章主要介绍了 OriginOS 提供的一系列搭载高安全级别保护功能的安全组件，如支付保护、信息验证码保护，安全键盘等，将这些安全组件融入到 vivo Pay、手机交通卡、eID 安全身份认证、手机车钥匙等应用中，能够最大程度地保障用户的个人隐私及财产安全。

5.1 高级别的安全功能

5.1.1 支付保护功能

OriginOS 提供的支付保险箱为支付类应用提供更高安全级别的保护。支付保险箱支持支付类应用在系统内独立的空间运行，免受外部应用程序的侵犯。

OriginOS 还提供支付环境的保护，即当用户启动支付类应用或进行支付时，系统会对当前的支付环境进行检测，当检测到安全风险时会及时提示用户，以降低用户的支付风险，提高用户防范意识。支付环境检测包括：

1 WLAN 安全检测

如果用户启动支付类应用或进行支付时使用 WLAN 连接方式，则 OriginOS 会判断当前 WLAN 网络是否存在网络攻击，主要检测方式包括 ARP 攻击检测、中间人攻击检测、DNS 服务器劫持检测等；

2 仿冒应用校验

对于当前进行的支付类应用，OriginOS 会检查该应用是否为仿冒的非官方应用，以防止用户在重打包的盗版仿冒应用上发生支付行为，造成用户的隐私泄露及财产损失；

3 恶意应用扫描

用户启动支付类应用或进行支付时，OriginOS 会扫描后台是否存在恶意应用程序企图介入干扰支付操作，保证支付行为不被恶意应用监听。

5.1.2 信息验证码保护功能

日常手机使用中，很多第三方应用在安装时会申请短信读取权限，用户首次授权后，很少关注后续此权限被长期授予的必要性，导致第三方应用可随时读取短信中的信息。而短信验证码作为一种有效且必要的人机识别手段，一旦泄漏不仅会对用户造成骚扰，甚至带来财产损失。

OriginOS 提供信息验证码安全保护功能，以减少验证码信息泄漏的风险。当用户接收新信息时，“信息”应用将对该短信文本进行解析，若判定为验证码，将禁止所有第三方应用读取和使用该验证码信息，避免出现用户误授权导致的信息泄漏风险。

5.1.3 安全键盘

安全键盘旨在对用户的密码输入提供安全保护，避免用户的密码信息泄露。启用安全键盘功能后，当系统检测到输入信息为密码类型时，自动启动 OriginOS 安全键盘（银行、支付类应用优先使用应用自有安全键盘）。OriginOS 安全键盘无任何本地和在线的联想及记忆功能，无法开启任何个性化功能，没有联网权限，不会收集用户的密码数据，更不会在系统剪贴板中缓存任何信息，最大程度地隐匿用户的输入行为，保障用户的输入安全。

5.2 高安全级别应用

5.2.1 vivo Pay

vivo Pay 是 vivo 钱包提供的手机支付服务。用户可以在支持 vivo 钱包的终端设备上，通过 vivo 钱包绑定银行卡，享受安全、便捷的支付体验，让手机成为银行卡。vivo Pay 可用于线上支付、线下 POS 机支付及地铁、公交出行等多种应用场景。

vivo Pay 的银行卡信息存储在金融安全级的安全元件中，可以通过 NFC 控制器与 POS 机进行交易，交易前手机会先通过指纹或密码验证用户身份。

退出 vivo 帐号时，vivo 钱包会将银行卡设置为不可用状态，即使手机处于无网状态，用户也可以联系发卡机构或支付网络，暂停或移除 vivo 钱包中银行卡的付款功能。用户还可以在 vivo 钱包中主动移除已添加的银行卡信息。

5.2.2 手机交通卡

vivo 手机交通卡是一种通过安全的方式将交通卡应用和数据下发到安全元件中运行和存储，实现手机交通卡的功能。

用户在开通了手机交通卡后，可以在手机上进行交通卡余额充值、刷卡交易、查询交通卡卡号、余额等卡片信息，也可以在云端和手机之间迁移交通卡、申请退还交通卡余额等。

5.2.3 eID 安全身份认证

eID 是由公安部第三研究所提供的安全认证技术，能够在各类线上和线下场景为用户提供身份识别和认证服务。

在 vivo 手机上加载 eID，借助智能手机的安全元件（SE）和可信执行环境（TEE）的安全机制，为用户提供高安全等级的认证服务和个人信息保护。

5.2.4 手机车钥匙

手机车钥匙是 vivo 和车辆厂商联合提供的数字钥匙服务。在开通手机车钥匙服务后，用户只需将手机与车辆碰一碰，即可完成开关车门、启动车辆等操作。通过车辆厂商的 App，车辆所有者可以授权亲友管理车辆并开通车钥匙，车辆所有者也可以随时撤消授权。使用手机车钥匙过程中涉及的钥匙信息和数字密钥等敏感信息存储在满足金融级安全标准的安全元件中，可以充分保护用户数字钥匙的安全。

06 云服务与设备管理安全

vivo 通过帐号保护功能以及一系列的帐号风控措施，并辅以安全有效的设备管理机制，来有效保证用户的信息安全。

6.1 vivo 帐号数据安全

对于 vivo 提供的所有在线服务（如 vivo 音乐、vivo 摄影专区等），用户均可以通过登录 vivo 帐号来访问。然而，在服务访问过程中，可能会存在第三方未获得用户授权就访问用户帐号的安全风险。为了消减此类风险，确保用户的数据和隐私安全，vivo 在用户帐号安全管理上采取了如下措施：

1 密码设置限制

用户设置密码时，密码的长度需要设置为 8 位及以上（最多为 16 位）、密码需要含有字母（包含大小写）和数字、且密码不能是较为常见的简单密码；

2 主动安全提醒

当用户帐号发生关键修改时，vivo 会及时主动地通过实时短信、消息提醒等方式告知用户；

3 帐号异常监测

若监测到有异常行为，vivo 会立刻提示用户对 vivo 帐号密码进行更改、在线申诉等，并提供快速自助冻结帐号服务，来保障帐号内的资产安全；

4 敏感信息加密存储

vivo 会对用户注册帐号的所有敏感信息进行加密存储，保证除了用户本人外，任何其他第三方都无法获取用户帐号的敏感信息；

5 安全的第三方登录

针对用户第三方授权登录，vivo 隐私中心也会将用户的授权信息进行加密，并且提供更改和取消第三方授权的能力；

6 随时永久性注销帐号

当用户选择注销帐号时，vivo 将彻底删除在线存储数据，以及访问、购买等所有关联数据。

6.2 vivo 帐号风控措施

vivo 提供了一系列的帐号风控措施来进一步地保障用户的帐号安全：

1 vivo 提供更加智慧的双重认证机制，即在保障帐号快捷登录使用的同时，风控系统会根据不同的使用场景，对帐号的登录进行双重验证；

2 vivo 提供的帐号设备登录服务，用户可以实时查看帐号的登录信息，若出现异常登录设备可将其移出；

3 当用户手机不在身边，或者手机号停机、换号，没有其他有效验证方式的情况时，vivo 将提供更加智慧的申诉系统，帮助用户找回密码或重置手机；

4 若风控系统识别到帐号存在密码泄露的风险，当用户再次登录帐号时，提醒用户必须要修改密码后才能正常使用。

vivo 智能风控系统基于全流程和全场景的风险识别机制和对抗机制，确保在用户注册、用户登录、访问与操作、密码找回、注销与冻结等帐号生命周期中用户信息的安全性。

6.3 vivo 设备管理

vivo 为用户提供了安全的设备管理服务，例如用户在设备遗失后，可以登录 vivo 云服务网站（cloud.vivo.com），通过内部“查找设备”的功能在地图上查看设备的当前位置。同时，vivo 还将提供诸如锁定屏幕、响警报音、数据备份、清除设备数据等设备管理服务，来全面保障用户数据的安全性。

07 数据安全

OriginOS 提供了密钥管理、密码保险箱、文件级加密（FBE）、TF 卡数据加密等功能，对用户数据进行加密保护；还提供了云数据加密存储备份服务，以保证用户数据备份的安全。

7.1 密钥管理

OriginOS 支持 Keystore 特性，对 Android 应用所使用的密钥和证书的全生命周期进行管理，密钥管理具有如下功能：

1 密钥生成和存储

OriginOS 支持硬件加解密能力，在可信执行环境（TEE）中根据应用指定的密钥类型生成对称密钥和非对称密钥，生成的密钥由 TEE 进行加密后存储。

2 密钥导入和导出

业务外部生成的密钥可通过安全的方式导入到 TEE 中的安全存储区域，并进行加密保护；另外也可以导出非对称密钥的公钥，来对其对应私钥签名的数据进行验签。

3 加解密服务

加解密服务提供密钥访问接口，应用通过该接口来使用对应密钥进行加解密操作，所有加解密操作均在 TEE 中执行。

4 密钥认证

每台 vivo 手机在生产时都注入了由 Google 公司颁发的证书，生成的密钥都可以使用 Google 的证书进行校验。在线认证时，密钥认证功能可以对 OriginOS 设备进行认证。

除了对应用所使用的密钥和证书的全生命周期进行管理外，Keystore 还增加了密钥提取防范和身份验证等安全功能，避免在 Android 设备之外以未经授权的方式使用密钥：

（1）密钥提取防范

为防止攻击者在 OriginOS 设备之外提取密钥，OriginOS 通过 Keystore 密钥执行加密操作时，应用会将待签署或验证的明文、密文和消息发送到执行加密操作的系统进程，而不是应用进程。因此，即使应用进程遭受攻击，攻击者也无法提取密钥材料。同时，OriginOS 将密钥绑定至 vivo 设备的安全硬件，密钥永远不会暴露于非安全世界。即使 OriginOS 操作系统遭受攻击或者攻击者读取到设备的存储空间，也无法从设备上提取这些绑定安全硬件的密钥材料。

（2）密钥使用的授权

为避免在 OriginOS 设备上以未经授权的方式使用密钥，在生成或导入密钥时，Keystore 会让应用指定密钥的授权使用方式。一旦生成或导入密钥，其授权使用方式将无法更改。以后每次使用密钥时，都会由 Keystore 强制执行授权。OriginOS 支持的密钥使用授权分为以下几类：

- 加密：授权密钥的算法、用途（如加密、解密、签名、验证等）、填充方案、分块模式以及摘要；
- 有效的时间间隔：密钥获得授权使用的时间间隔；
- 用户身份验证：只有用户在最近一定时间段内成功地进行了身份认证时，密钥才能使用。

7.2 云服务数据备份

OriginOS 云服务提供实时的数据同步和备份功能。用户将手机中的通讯录、短信、相册等信息同步备份至 OriginOS 云服务后，云端会对用户数据的存储进行分区，并使用密钥长度至少为 128 位 的 AES 算法单独加密文件区块，保证云端用户数据的安全性。

7.3 文件级加密

OriginOS 支持 Android 的文件级加密（FBE，File-Based Encryption），能对每一个文件使用不同的密钥进行加解密，即支持对每一个文件进行单独加解密。基于文件级的数据加密，可以防止未经授权的用户获取其他用户私密数据，为用户隐私提供更好的安全保障。

在 OringinOS 支持的 FBE 设备上，用户有两种存储空间：

1 凭据加密（CE）存储空间

默认存储位置，只在用户解锁设备后才可用；

2 设备加密（DE）存储空间

在开机启动期间以及用户解锁设备后均可用；

OriginOS 使用凭据加密（CE）存储空间作为默认存储位置，确保应用和数据在用户解锁设备后才能使用；同时将闹钟、铃声、短信等部分应用数据保存在设备加密（DE）存储空间，使得这些应用可以在设备解锁之前进行数据访问，既保障了必要应用的使用，同时也能保护用户私密信息。

7.4 密码保险箱

密码保险箱是vivo为用户打造的本地密码管理工具，可以实现网页端（仅支持系统浏览器）的帐号密码与其应用端帐号密码统一保存管理，并且和指纹识别或锁屏密码相关联。密码保险箱还支持本地内置名单自动关联聚合家族应用登录信息，即用户在网页端（仅支持系统浏览器）和应

用端登录时会自动填充登录信息，方便用户使用。

基于可信执行环境实现的密码保险箱，提供了硬件级加密存储能力，“密码”数据对应的加密密钥在 TEE 内保存，且“密码”数据的加解密操作始终在 TEE 内执行。

密码保险箱保存的帐户密码数据在用户授权后，能在支持密码保险箱的 vivo 终端设备之间，通过互传的方式进行加密传递。

7.5 TF 卡数据加密

TF 卡数据加密是通过与移动设备绑定的方式对 TF 卡内的数据进行加密保护。在启用 TF 卡加密功能后，TF 卡将和移动设备建立绑定关系并加密 TF 卡内所有数据。TF 卡内加密后的数据只有该移动设备才能正确解密读取，其它支持 TF 卡接口的设备将无法读取正确的数据。

7.6 数据删除

OriginOS 提供了两种恢复出厂设置删除数据操作。第一种是清除所有数据但未勾选格式化手机存储，此操作会删除应用相关数据，而用户存放在手机存储中的私密数据（比如：音乐、视频、图片等）则会保留。

为确保用户的应用数据和私密数据均被删除，OriginOS 也将提供第二种恢复出厂设置删除数据的操作，即清除所有数据并勾选格式化手机存储。此操作会格式化整个用户存储空间的数据，并删除用户数据的逻辑地址，确保数据删除后不可见，保证用户的数据安全。

08 隐私保护

OriginOS 在隐私保护方面，始终坚持透明可控、隐私端侧处理、数据最小化的原则。属于用户的内容该如何呈现和使用，均由用户自己决定；通过机器学习在设备端侧完成的任务，尽可能在本地进行；为实现功能服务而必须向用户收集的数据，也保证只会最小限度地获取。

8.1 权限管理

OriginOS 系统提供了权限管理机制，以限制应用程序的敏感操作，保护用户隐私数据。如果应用程序在运行时需要访问用户隐私数据，应用程序会向用户发出权限申请请求，最终由用户决定授予或不授予所申请隐私数据的访问权限。权限的细粒度管理会持续改进和优化，OriginOS 允许用户针对某个权限进行允许 / 禁止等操作。权限管理功能支持如下资源的访问控制：电话、短信、联系人、通话记录、相机、定位、麦克风、日历、传感器、身体活动、存储等。

8.2 定位隐私保护

位置信息是重要的用户隐私数据。针对常见的四种定位方法：GPS、WLAN、蓝牙、基站信息，OriginOS 在设置中提供统一的定位服务开关，关闭开关后，将同时关闭四种定位功能，充分保护用户的位置隐私数据。另外，针对不同的场景，用户可选择“始终允许”、“仅使用时允许”、“每次询问”、“禁止”四种位置权限授予方式：

1. “始终允许”：应用在前后台都可以获取位置信息；
2. “仅使用时允许”：应用在后台模式中无法获取位置信息；
3. “每次询问”：应用每次尝试获取位置信息时询问用户；
4. “禁止”：应用无法获取到位置信息。

8.3 录音录像隐私保护

为了避免恶意应用通过欺骗的方式获取麦克风 / 相机权限后，在用户不知情的情况下进行录音 / 录像，窃取用户的隐私数据，OriginOS 提供了录音录像提醒功能。当应用程序使用麦克风或者摄像头时，系统会在状态栏提醒用户有应用正在使用麦克风或者摄像头。用户下拉状态栏点击相应提示时，会以弹窗形式显示当前正在使用相应权限的应用。用户也可以点击提示中的关闭按钮，关闭正在录音 / 录像的应用。

8.4 标识符体系

为了防止应用通过设备标识符对用户进行追踪，OriginOS 采用了设备匿名化标识符体系，从而禁止第三方应用获取设备的永久性设备标识符，如 IMEI、SN、MAC 地址（Media Access Control Address）等。

根据不同的使用对象和不同的使用用途，OriginOS 支持生成四类标识符，即设备唯一标识符（UDID）、匿名设备标识符（OAID）、开发者匿名设备标识符（VAID）和应用匿名设备标识符（AAID），这四类设备标识符之间不存在映射关系。应用发送获取设备标识符的请求时，OriginOS 会对应用进行验证，并验证其请求是否符合策略规定，然后将相应的标识符返回给应用。

8.5 防截屏录屏

OriginOS 为用户的密码输入界面提供了防止截屏、录屏的功能。在用户触发密码输入界面时，如果第三方应用进行截屏，则拒绝触发截屏操作；如果第三方应用进行录屏，则录制的界面始终会保持在开始输入时的界面，从而防止用户敏感信息的泄漏。（目前仅支持 EditText 的输入密码界面，其他输入密码界面不会拦截。）

8.6 隐私密码

为确保用户信息内容的私密性与安全性，防止因个人信息泄露而引发的隐私权益无法保障、个人财产损失等，OriginOS 采用了独立的隐私密码体系。隐私密码体系是一套独立且安全的隐私验证体系。通过将隐私密码体系应用于通信内容、便签内容、应用加密及原子隐私系统等功能，以此解决用户在各个使用场景下的隐私泄漏问题。

8.7 原子隐私系统

原子隐私系统提供了一套系统级的隐私保护解决方案。它具有便捷可控的本地化存储和管理能力，可以将图片、视频、音频、文档等文件或应用移入到原子隐私系统内安全地存储。文件和应用移入原子隐私系统后，用户需要验证指纹或隐私密码才可进入并查看数据，保证数据安全。

8.8 摄像头检测

为了保护用户的个人隐私，防止用户被隐藏的摄像头偷拍，OriginOS 在 i 管家中提供了摄像头检测功能。该功能允许用户使用网络检测或手动检测方式，检查房间里是否安装偷拍摄像头。网络检测通过对当前网络的多维度数据分析来识别网络摄像头，而手动检测可以通过物理的光学原理检测到摄像头的安装位置，保护用户隐私。

8.9 差分隐私

差分隐私是通过在个体数据中添加随机噪声，然后结合大量的添加过随机噪声的用户数据，借助差分隐私算法消除所添加的随机噪声，获得所需的相关信息。因此，差分隐私能在隐藏用户的个体信息、保护个人隐私的前提下，帮助业务获得所需信息。基于差分隐私技术，OriginOS 能够在保护个人隐私的同时，在可靠性、性能、功耗等方面进行持续改进和优化，为用户提供更极致的使用体验。

09 安全标准遵从与认证

vivo 作为一家以消费者需求为核心导向的公司，始终将消费者安全与隐私保护放在首位，严格遵循相关安全标准，目前在安全和隐私保护方面已获得多项国际和国内权威认证。其中，vivo 互联网服务遵循网络安全等保保护要求，已经通过网络安全等级保护三级。

OriginOS 获得了中国泰尔实验室首张移动智能终端操作系统个人信息保护能力五星产品的证书。

ISO/IEC 27001 Information Security Management CERTIFIED

ISO/IEC27001 由国际标准化组织和国际电工委员会联合发布的信息安全管理体系 (ISMS) 标准，通过认证表明企业已经建立并有效运行信息安全管理体系，满足内外部信息安全管控要求。

TRUSTED PRIVACY P ePrivacy

由欧洲隐私认证权威机构 ePrivacy 颁发，涵盖了数字产品的通用数据保护法规（GDPR）的要求，从法律和技术两个维度对认证对象进行评估，确保覆盖 GDPR 法律要求。“i 管家”与“vivo 相册”欧洲版本通过审查并取得认证。

ISO/IEC 27701 Privacy Information Management CERTIFIED

ISO/IEC27701 由国际标准化组织和国际电工委员会联合发布，为建立、实施、维护和持续改进隐私信息管理系统提供具体要求和指南。通过认证表明企业隐私信息管理体系和隐私保护能力满足国际标准。

TRUSTe Certified Privacy Powered by TrustArc

基于各国公认的法律和法规标准，由国际权威隐私合规评估机构 TrustArc 颁布。通过认证表明企业满足国际级隐私保护的认证标准，相关技术和管理能力获得美国隐私认证权威机构 TrustArc 的认可。

OriginOS

10 术语表

英文缩写	英文全称	中文全称
3DES	Triple Data Encryption Algorithm	三重数据加密算法
AAID	Application Anonymous Device Identifier	应用匿名设备标识符
AES	Advanced Encryption Standard	高级加密标准
AI	Artificial Intelligence	人工智能
API	Application Programming Interface	应用软件编程接口
ARP	Address Resolution Protocol	地址解析协议
CE	Credential Encrypted	凭据加密
CPU	Central Processing Unit	中央处理器
DE	Device Encrypted	设备加密
DNS	Domain Name Server	域名系统
ECDSA	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名算法
eID	electronic IDentity	公民网络电子身份标识
FBE	File-Based Encryption	文件级加密
GPS	Global Positioning System	全球定位系统
HMAC	Hash-based Message Authentication Code	散列消息认证码
HUK	Hardware Unique Key	设备唯一密钥
IMEI	International Mobile Equipment Identity	国际移动设备识别码
KASLR	Kernel Address Space Layout Randomization	内核地址空间布局随机化
MAC	Message Authentication Code	消息认证码

英文缩写	英文全称	中文全称
MAC	Mandatory Access Control	强制访问控制
MAC	Media Access Control Address	MAC 地址
NWS	Normal World Status	非安全世界
OAID	Open Anonymous Device Identifier	匿名设备标识符
OriginOS	OriginOS	vivo OriginOS 系统
OTA	Over The Air	空中下载技术
PIN	Personal Identification Number	个人身份识别码
PAN	Privileged Access Never	特权模式访问禁止
PXN	Privileged Execute Never	特权模式执行禁止
REE	Rich Execution Environment	富执行环境
RPMB	Replay Protected Memory Block	重放保护内存块
RSA	Rivest Shamir Adlem	公开密钥密码体制
SE	Secure Element	安全元件
SELinux	Security Enhanced Linux	安全强化 Linux
SFS	Secure File Syste	安全文件系统
SHA	Secure Hash Algorithm	安全散列算法
SN	Serial Number	序列号
SoC	System on Chip	片上系统
SWS	Secure World Status	安全世界
TA	Trusted Application	可信应用
TEE	Trusted Execution Environment	可信执行环境
TF	Trans FLash	内存卡
TUI	Trusted User Interface	可信用户交互
UDID	Unique Device Identifier	设备唯一标识符
UID	User Identify	用户 ID
VAID	Vender Anonymous Device Identifier	开发者匿名设备标识符
WLAN	Wireless Local Area Network	无线局域网络