

华为技术有限公司
深圳龙岗区坂田华为基地
电话: +86 755 28780808
邮编: 518129
www.huawei.com

华为产品安全基线白皮书

华为网络安全管理实践



商标声明

 HUAWEI, HUAWEI,  是华为技术有限公司商标或者注册商标，在本手册中以及本手册描述的产品中，出现的其它商标，产品名称，服务名称以及公司名称，由其各自的所有人拥有。

免责声明

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺，华为不对您在本文档基础上做出的任何行为承担责任。华为可能不经通知修改上述信息，恕不另行通知。

版权所有© 华为技术有限公司 2021。保留一切权利。

未经华为技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。



目 录

1. 前言	01
2. 执行概要	02
3. 产品安全是网络安全的关键因素	03
4. 安全需要嵌入产品成为产品的基础能力	04
5. 产品安全基线在业务流程中的应用	04
6. 华为制定并刷新产品安全基线的原则	07
· 它是基于结果的	07
· 它是普遍适用的	07
· 它是无差别的	07
· 它是持续优化的	07
7. 华为产品安全基线介绍	08
保护用户通信内容	09
保护用户隐私	09
防止后门	09
防止恶意软件、恶意行为	09
访问通道控制	09
系统加固	09
应用安全	10
加密	10
敏感数据保护	10
管理和维护安全	10
安全启动和完整性保护	10
安全资料	11
安全编码	11
安全编译	11
生命周期管理	12
8. 总结	12

1. 前言

2020 年，新冠疫情改变了组织的运作模式和人们的生活方式，很多线下行为被迫转为线上，远程办公、视频会议、远程教育、远程医疗等成为新常态。数字技术在确保社会生活、企业运行连续性方面发挥了无可替代的作用。但数字化的加速发展也进一步加剧了网络安全和隐私保护的挑战，2020 年全球安全漏洞和网络攻击的数量和规模都创历史新高，勒索病毒、数据泄露事件层出不穷。在 5G、云和 AI 使能的数字化智能世界，安全稳定的网络空间对国计民生至关重要，网络安全和隐私保护越来越成为数字世界的内生需求和基础能力。

面对网络空间的挑战，提升网络安全水平，既是政府 / 监管机构、行业 / 标准组织、通信网络服务提供商、通信技术供应商、提供数字化服务的企业等数字空间内所有利益相关方的共同责任，也是各方通过加强合作，提升网络安全、推进数字化进程的机遇。在面对网络攻击，网络空间上各供应商提供的所有产品、所有服务都会暴露在攻击面上，只有提高端到端的全供应链的网络安全防护水平，才能有效地削减整个网络的安全风险。

华为是全球领先的 ICT 基础设施和智能终端提供商，产品种类繁多、形态多样、应用场景千差万别，如何有效管理这些产品的安全是个巨大挑战。华为将网络安全管理要求融入到内部各业务流程中。在集成产品开发 IPD 流程中，将产品网络安全要求融入到从规划、设计、开发、验证、版本发布到全生命周期管理的整个过程中，保障了华为交付给客户的全系列产品和版本都能满足各利益相关方关注的安全质量要求。在这些管理要求、工程与技术规范中，华为产品安全基线是强制性的基础要求。基于过去十多年华为在产品安全质量上的长期实践，我们持续不断的优化、刷新这一产品安全基线，也和合作伙伴、供应商等共同分享这个安全基线对保障端到端供应链安全所带来的价值。实践表明，华为产品安全基线不仅能够适用于华为产品，同时也适用于华为的供应链。华为持续十多年的安全实践也证明了，产品安全基线是一个有效管理产品安全质量的方法，也保障了华为产品在客户网络上一直以来良好的安全运行记录。

注：华为产品安全基线描述了为保障华为产品达到一定的安全能力而必须满足的要求，它是保障产品安全的要求的子集，当然，这些要求并不是为了保障产品安全相关的所有要求。

华为在这10年间也在持续不断更新华为产品安全基线，以应对面临的现有的和不断新出现的威胁，因此，除非另有明确说明，每次更新的要求可能仅应用于发布更新要求之后的新开发的产品中。

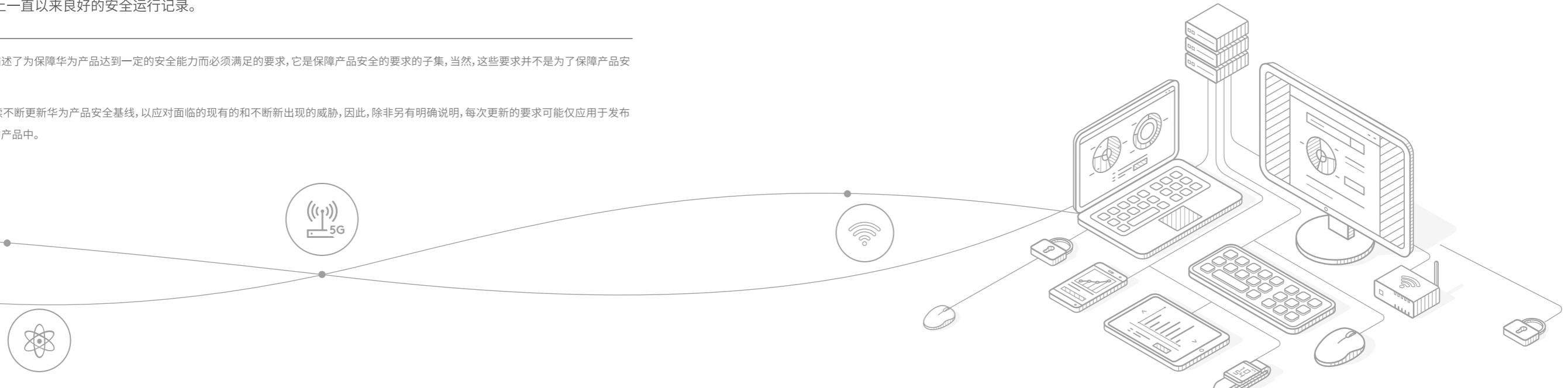
2. 执行概要

我们认为：

- 面对安全事件频发的全球网络安全现状，提升产品自身安全是关键的风险削减措施之一。
- 将安全管理嵌入到产品开发过程中，使网络安全成为产品的基础能力之一，才能从根本上解决网络安全问题。
- 提炼基础的、通用的产品安全基线要求，并在所有产品中落地，可以确保所有产品都能达到一致的安全质量基础要求，并随着基线的刷新而不断提升产品安全质量。
 - 在华为端到端的网络安全框架下，华为产品安全基线作为基本的安全要求，嵌入产品开发流程，通过严格的质量保证活动，确保产品安全质量，减少发生安全事故的风险。

华为产品安全基线：

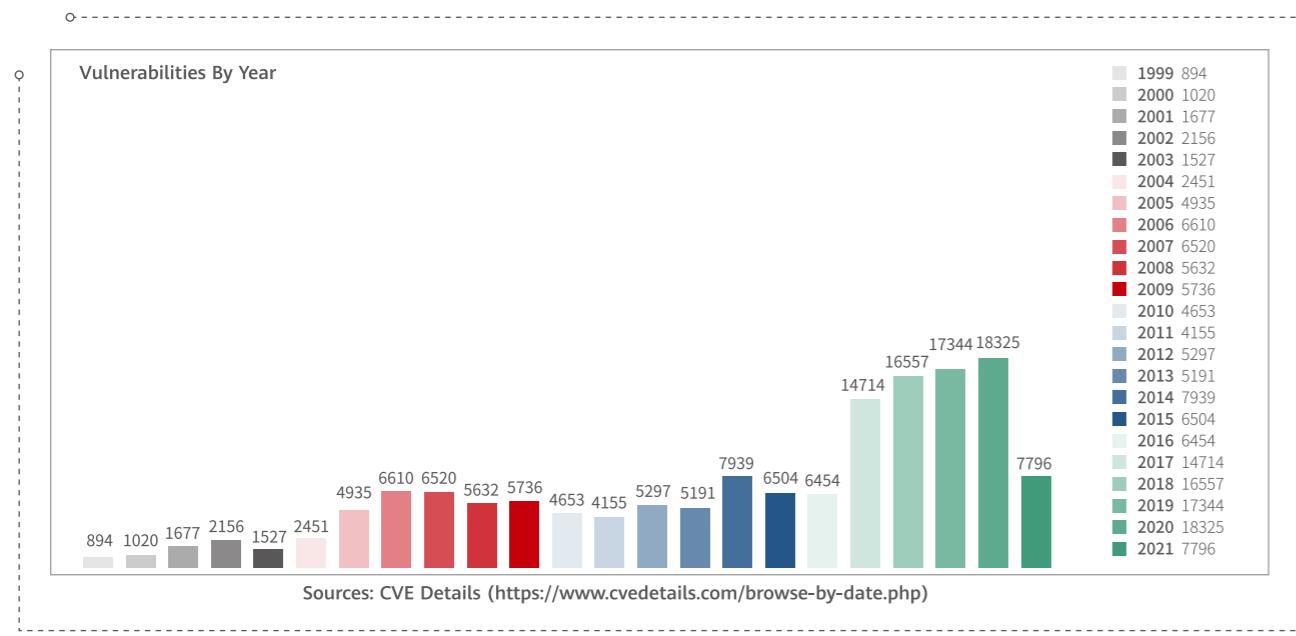
- 华为以“基于结果、普适、无差别、持续优化”为原则，制订华为产品安全基线，保证了华为产品安全基线的有效落地、可验证和可持续提升产品安全质量水平。
- 通过研究适用法律法规，深入理解法律合规要求、客户业务诉求、业界最佳实践、行业内已知问题等，识别出产品通用的、最关键的安全要求，制定了华为产品安全基线。华为产品安全基线涵盖 15 个类别、54 条要求，相关的实施指导与解读共计 112 条。



3. 产品安全是网络安全的关键因素

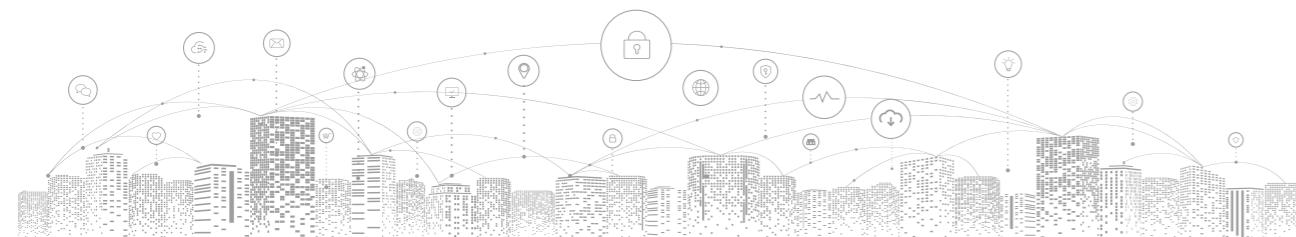
随着 5G 和数字化的深入发展,无人驾驶、智慧城市、智能工厂全面普及,人人互联、机机互联,甚至人机互联成为可能。数字化推动了经济的发展,给我们的生活带来天翻地覆的变化,同时,数字化模糊了传统的网络物理边界,使得网络风险和威胁也与日俱增,漏洞和攻击造成的后果也更加严重。

全球网络安全事件频发,2006 年曝光的希腊监听事件,2010 年震网 (STUXNET) 病毒,2014 年心脏滴血漏洞 (HEARTBLEED),2017 年全球爆发永恒之蓝勒索蠕虫 (WANNACRY),2018 年处理器芯片“MELTDOWN”和“SPECTRE”漏洞……究其原因,产品本身的安全是关键因素之一。



如上图,从历年的 CVE 漏洞数据统计¹ 我们可以看到,从 2017 年开始,每年的安全漏洞数量都超过了 1.4 万个,连续四年每年的安全漏洞数量屡创新高。随着系统变得更加复杂,不断出现和发展的新软件框架和技术,以及使用更多的开源和第三方组件等等因素,使得影响产品安全的因素越来越多、越来越复杂,产品安全风险持续增长,产品的安全越来越得到全行业的关注和重视。

注1: 2021年6月2日的漏洞统计数据, <https://www.cvedetails.com/browse-by-date.php>



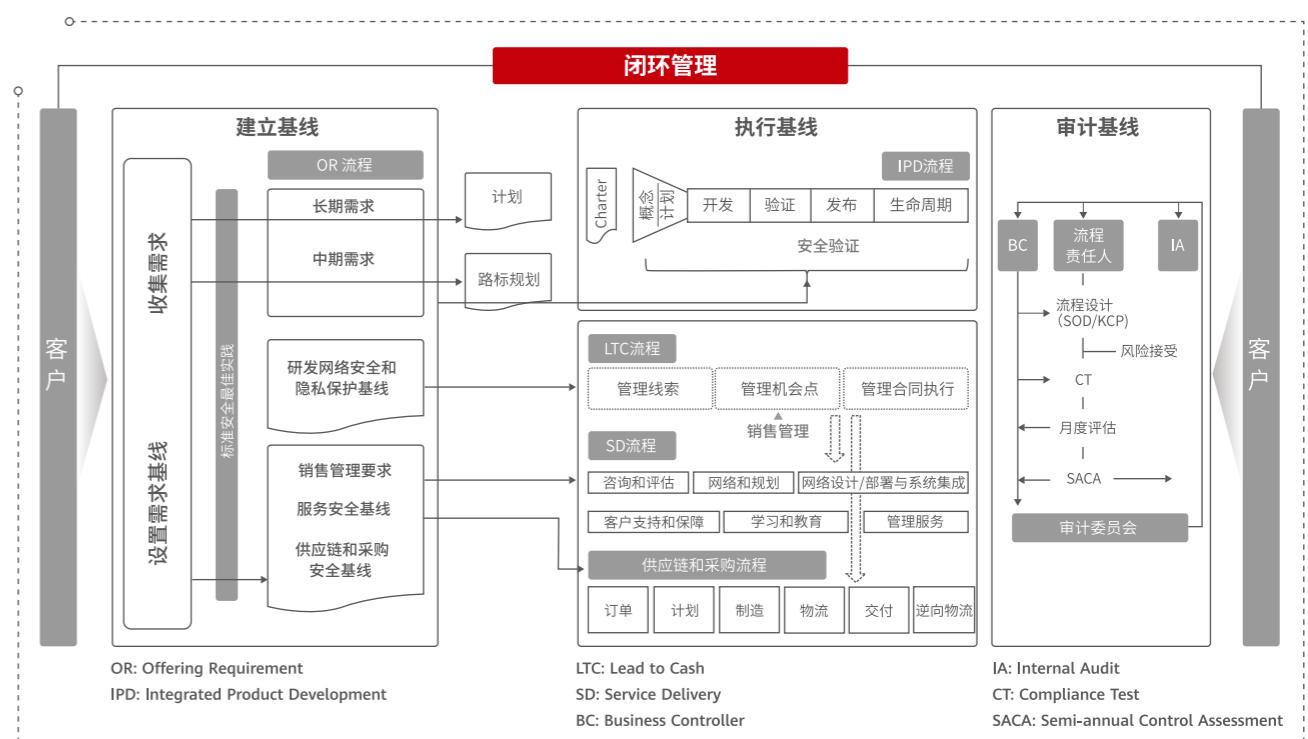
4. 安全需要嵌入产品成为产品的基础能力

传统的边界防御,采用叠加防火墙、安全软件、入侵检测等安全产品来保护网络与系统安全的方法,已经不足以面对复杂的安全场景和安全形势。如果产品本身安全质量不高,存在大量潜在安全漏洞的风险,即使进行及时的漏洞修复这种有效的风险缓解措施,也无法应对当前网络安全的挑战。

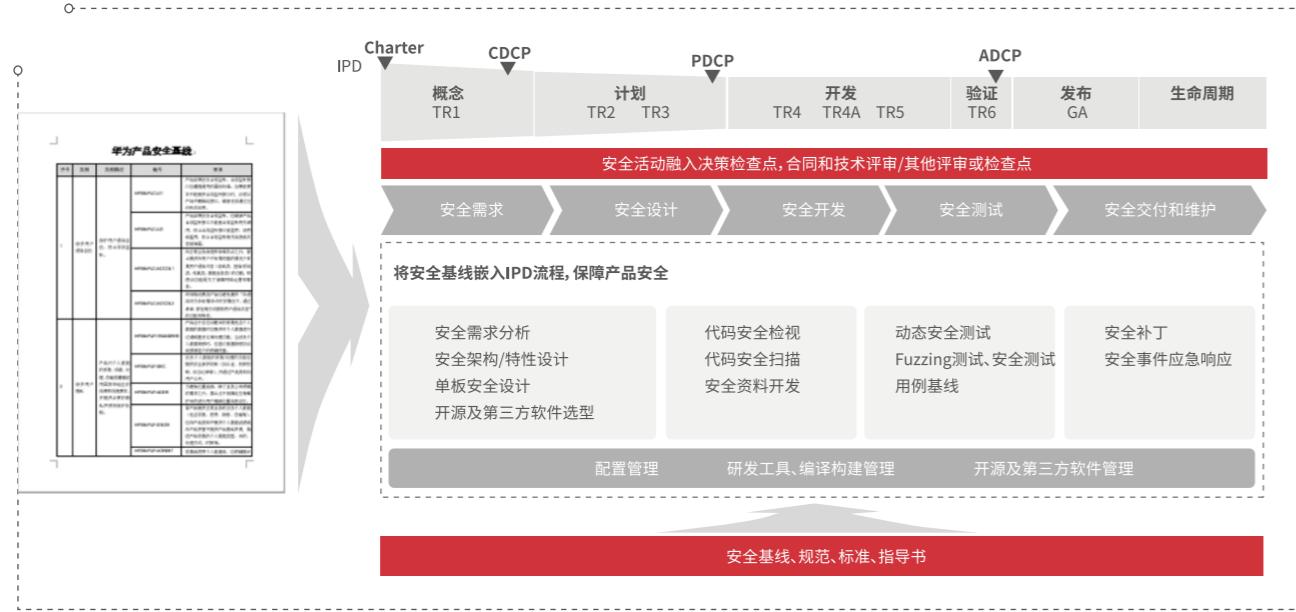
如今,行业界已经形成共识,Security By Design,安全与产品是一个整体,安全是内生的而不是叠加的,安全防护不仅需要“发现风险、查漏补缺”,更需要“防护前移、系统规划”。在产品规划设计的初期就要把安全规划做进去,在整个开发和产品生命周期中通过系统性的规划与设计来实现安全、保障安全。将安全嵌入产品成为产品的基础能力,才能有效地解决安全问题,同时达到节省时间并降低成本的效果。

5. 产品安全基线在业务流程中的应用

华为致力于提供安全可靠、高质量的 ICT 通信基础设施,网络安全是我们的最高纲领。通过长期的投入和探索,华为打造了端到端的网络安全框架(见下图),通过安全基线,在全业务流程中对产品安全实现有效管理。



在产品安全管理上,我们提炼出产品通用的、最关键的安全要求作为基线并在所有产品中落地,以确保所有产品都能达到一致的安全质量要求,并随着基线的持续刷新而不断提升产品安全质量水平。作为华为端到端网络安全保障框架的重要组成部分,华为产品安全基线涵盖 15 个类别、54 条要求,参考了广泛的外部法规、技术标准、监管要求,并通过华为的产品开发实践,保障了华为交付给客户的全系列产品和版本都满足各利益相关方关注的安全基础质量要求。

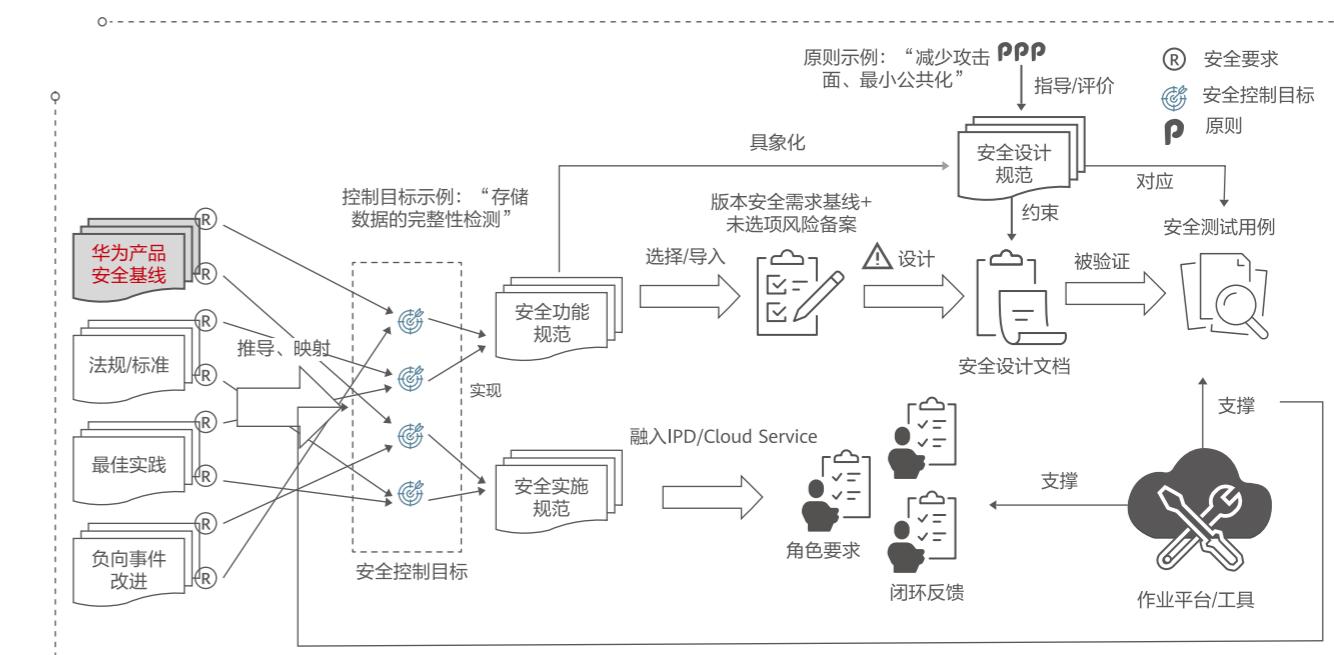
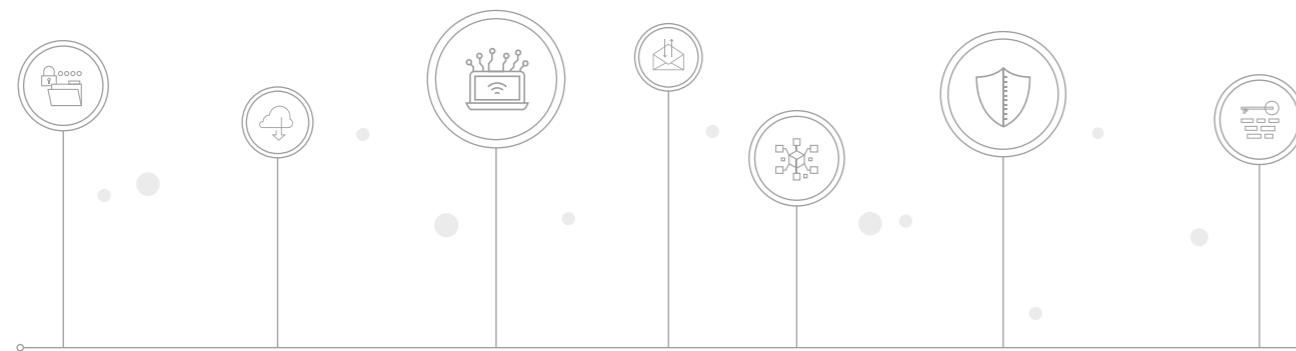


如上图所示,华为产品安全基线作为基本的安全要求,嵌入华为产品开发流程(IPD),从而可重复执行,而非随机执行。华为产品安全基线贯穿于产品的整个生命周期,执行 IPD 流程的相关角色和组织必须严格执行并落实华为产品安全基线。

1)首先,全球网络安全与用户隐私保护官 / 全球网络安全与用户隐私保护办公室负责华为产品安全基线的制定、发布及持续优化。通过评估法律、行业标准、业界最佳实践、客户要求、行业已知案例分析和网络安全技术最新发展,识别其中的最关键要求,持续更新华为产品安全基线;

2)各领域刷新相关的政策、流程和程序,与更新的华为产品安全基线保持一致;

3)研发以华为产品安全基线为作为关键输入之一,制定 / 刷新华为内部的技术标准、规范、模板、指南,并提供必要的培训和安全意识教育,以规范和指导产品设计和开发;



如上图所示,我们将华为产品安全基线等同于外部合规要求,通过将华为产品安全基线、外部法规 / 标准要求以及内外部最佳实践提炼和融入到华为内部规范,成为产品研发需要遵从的规范,高效、有序地帮助产品建立安全能力;

4)各业务部门落实华为产品安全基线,并在业务体系和决策体系进行评审、决策、执行和监控,对违反华为产品安全基线的行为进行回溯和问责;

5)在产品版本发布前,内部独立的网络安全实验室(ICS)负责以客户视角验证产品是否满足华为产品安全基线,对于不满足的版本,全球网络安全与用户隐私保护官对其发布拥有否决权;

6)对发现的问题,进行闭环管理,循环改进华为产品安全基线以及相应的管理机制。



6. 华为制定并刷新产品安全基线的原则

为了保证华为产品安全基线的有效落地、可验证、可持续提升产品安全质量水平，我们在制定和管理华为产品安全基线遵循以下原则：

它是基于结果的

只有结果性的要求才真正是客观的、可验证的，基于结果的产品安全要求有助于产品准确地实现预期目标，也有助于客户基于客观结果比较和选择所需的产品。

它是普遍适用的

进入华为产品安全基线的要求须是通用的、普适的，能够适用所有或者绝大部分产品、适用于多种业务场景，以确保华为所有产品都能达到一致的安全基础质量要求。

它是无差别的

我们处在全球供应链的时代，如果我们要真正确保所有系统和所有基础设施的安全，就应该对所有的供应商（无论在哪里开发、或者在哪里生产）、所有的产品部件（无论产品被应用于哪个区域、哪个网络、或者网络的哪个位置）采取同样的安全基础标准。

它是持续优化的

网络安全是一个动态的过程，华为产品安全基线须持续定期刷新，以适应不断发展的网络安全形势。



7. 华为产品安全基线介绍

通过对法律法规、标准规范、安全实践等的分析总结，提炼产品共同的、最关键的安全要求，华为制定了《华为产品安全基线》，并随着网络安全的发展和华为的实践持续刷新，最新版为2020年刷新发布的《华为产品安全基线V3.0》。

华为产品安全基线	
1.保护用户通信内容	4条
2.保护用户隐私	7条
3.防止后门	5条
4.防止恶意软件、恶意行为	2条
5.访问通道控制	5条
6.系统加固	4条
7.应用安全	3条
8.加密	5条
9.敏感数据保护	4条
10.管理和维护安全	5条
11.安全启动和完整性保护	2条
12.安全资料	3条
13.安全编码	2条
14.安全编译	1条
15.生命周期管理	2条

如上图，华为产品安全基线共计15类54条要求，为了便于华为众多产品以及不同应用场景准确理解和执行安全基线，同时还开发了实施指导与解读共计112条。

保护用户通信内容

用户通信内容受各国法律保护,华为在产品设计中严格遵循行业通用安全标准,确保通信数据安全。

保护用户隐私

华为分析了欧洲 GDPR、德国、法国、英国、加拿大、中国等国家的隐私保护法律法规要求,参考 GSMA 隐私设计规范等业界实践,按照“合法、正当、透明”、“目的限制”、“数据最小化”、“准确性”、“存储期限最小化”、“完整性与保密性”、“可归责”等 7 条隐私保护基本原则用于指导产品设计和开发。

防止后门

华为不允许在产品中植入后门,也不允许其他人在华为设备中植入后门。

防止恶意软件、恶意行为

华为不允许产品存在病毒、木马等恶意软件,也不允许产品存在恶意广告、吸费、恶意消耗流量等恶意行为。

访问通道控制

采用隔离、认证等手段控制访问通道,能够有效降低攻击面,保证接入产品访问的安全。

系统加固

通过安全配置、补丁修复漏洞、删除或禁用不必要的服务等方法,对产品进行安全加强以提高产品的安全性和抗攻击能力。

应用安全

WEB 应用、移动应用等各种应用容易受到黑客和恶意软件的攻击,导致未经授权的访问和修改,认证和鉴权是最基本的安全保护机制。

加密

密码算法是安全的基石,正确地使用密码算法是产品安全性的基石。根据不同应用场景使用密码算法,须使用公开的、经过专业评审和验证过的安全的密码算法,并正确地配置算法参数和选项。

敏感数据保护

在产品设计时,需要根据产品的使用场景,识别出产品中的敏感数据,典型的敏感数据包括认证凭据(如口令、私钥、动态令牌卡)、加密密钥、敏感个人数据(如银行账号、用户通信内容)等,从敏感数据的存储、传输和处理过程中采取认证、授权或加密等安全机制保证数据安全。

管理和维护安全

产品的管理维护采用严格的账号口令、安全的访问协议、完整的日志审计等安全机制,保证产品管理维护操作的安全。

安全启动和完整性保护

在产品的安装、升级中验证软件包的完整性,防止产品被攻击者恶意篡改。对于客户需要有高安全要求的产品同时考虑在启动过程中进行安全启动验证。

| 安全资料

产品的资料需要提供产品的通信矩阵、账号清单、安全加固和配置指南等安全资料，以便能够指导客户以最安全的方式使用、部署和维护产品。

| 生命周期管理

产品软件需要使用安全记录良好并持续维护的开源和第三方组件，出现漏洞及时通过发布补丁或者升级到新版本等方式修复漏洞，确保产品软件在生命周期内的安全处于可维护状态。

| 安全编码

大部分安全漏洞很大程度上是由于代码编写的不规范、编程语言特性理解不当、接口调用不当等代码质量缺陷导致的，通过例行的静态代码安全和质量扫描，以及减少不安全函数的使用，可以提前识别代码中的安全质量缺陷，持续提升代码质量，减少潜在的安全漏洞。

| 安全编译

编译器提供了相当多的安全选项来加固软件的安全性，通过添加安全编译选项，可以在软件中进行代码质量的安全加固，提高了攻击者的攻击难度，降低了代码质量缺陷变成可被利用漏洞的风险。

8. 总结

面对网络空间的挑战，提升网络安全水平，既是政府 / 监管机构、行业 / 标准组织、通信网络服务提供商、通信技术供应商、提供数字化服务的企业等数字空间内所有利益相关方的共同责任，也是各方通过加强合作，提升网络安全、推进数字化进程的机遇。

实践表明，华为产品安全基线是我们管理网络安全行之有效的方法之一，保障了华为产品在客户网络上一直以来良好的安全运行记录。华为愿意与利益相关方，包括运营商、企业客户、供应链的上下游合作伙伴、政府监管机构，围绕产品安全基线，围绕具体的安全管理、工程与技术规范、测试与验证方案等细节做进一步的深入沟通和讨论，持续优化华为产品安全基线，促进端到端供应链网络安全的水平。

网络安全的努力没有终点，Security, We Do More。

