海康威视网络安全白皮书

HIKVISION Cybersecurity White Paper

关于本文档

《海康威视网络安全白皮书》旨在概览海康威视针对智能物联领域网络安全进行的探索与实践，以开放透明的视角让广大用户全面了解海康威视的安全策略与能力。

海康威视可能对本文档进行更新，最新版将发布于公司官网（https://www.hikvision.com/cn/）。

版权声明

商标声明

海康威视、HIKVISION为海康威视的商标或注册商标。本文档中提及的其他公司名称或商标由其各自所有者拥有。

责任声明

在法律允许的最大范围内，本文档所述内容均“按照现状”提供，海康威视不提供任何明示或默示保证，包括但不限于适合特定目的、商用性等保证。

海康威视不保证本文档内容的精确性，并保留对其进行纠正或修改的权利，不另行通知。

任何使用或信赖本文档的内容而做出的决定及因此造成的后果由行为人自行承担。

如本文档中所述内容与适用的法律相冲突，则以法律规定为准。

修订记录

首次发布于 2018 年 1 月，于 2023 年 9 月第二次修订，于 2026 年 1 月第三次修订。

关于海康威视

海康威视成立于 2001 年，是一家专注技术创新的科技公司。

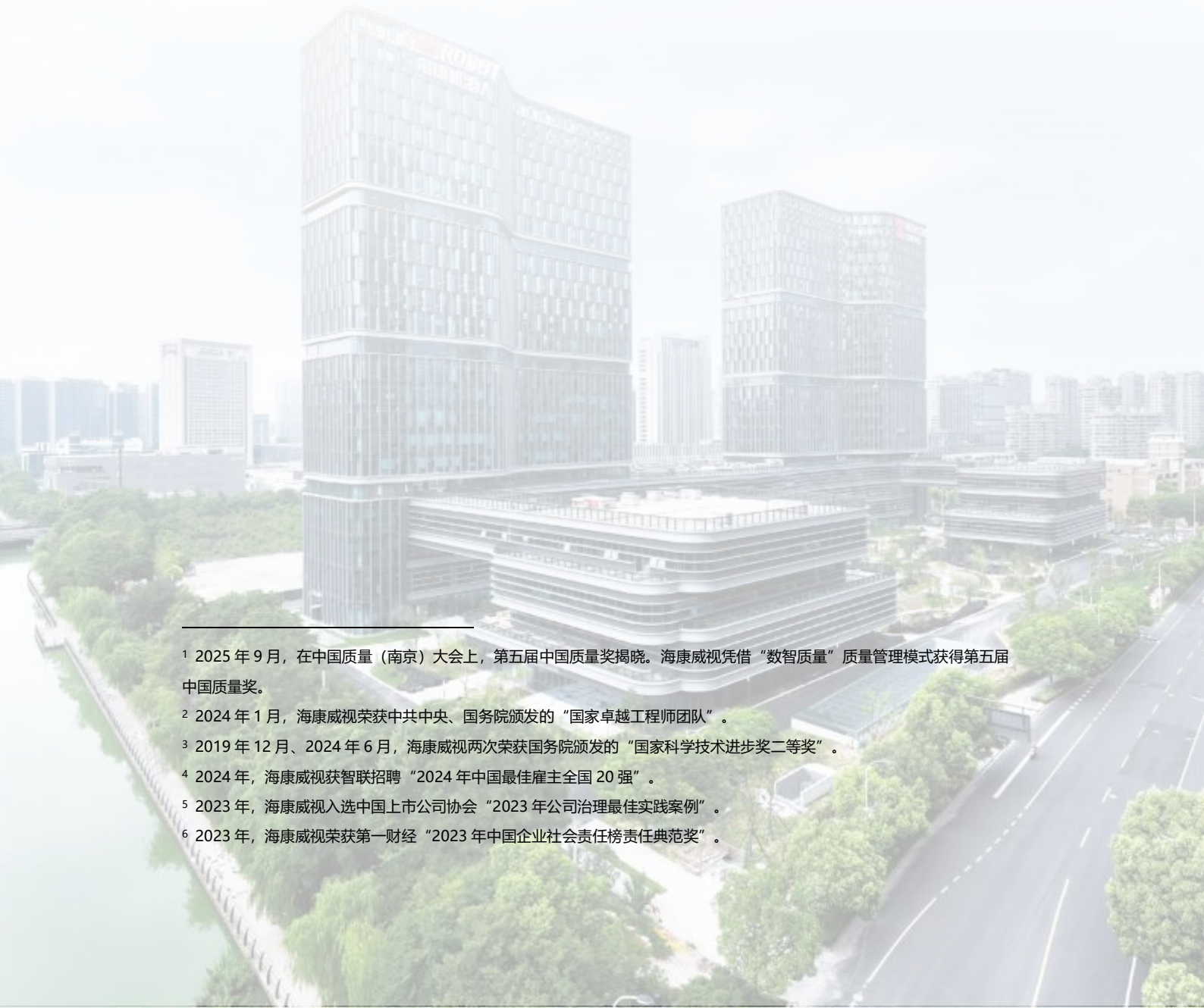
秉承“专业、厚实、诚信”的经营理念，践行“成就客户、价值为本、诚信务实、追求卓越”的核心价值观，二十余年来，海康威视以视频技术为起点，逐步构建和完善以物联感知、人工智能、大数据为核心的智能物联技术体系，为千行百业提供安防和场景数字化产品与服务。公司的产品和技术，已在杭州亚运会、G20 杭州峰会、北京奥运会、上海世博会、APEC 会议、北京大兴机场、港珠澳大桥等重大项目中发挥了重要作用。

海康威视致力于将物联感知、人工智能、大数据技术服务于千行百业，引领智能物联新未来：以全面的感知技术，帮助人、物更好地链接，构筑智能世界的基础；以丰富的智能产品，洞察和满足多样化需求，让智能触手可及；以创新的智能物联应用，建设便捷、高效、安心的智能世界，助力人人享有美好未来。

公司现有员工 59,689 人（截至 2024 年末），其中研发人员和技术服务人员 28,272 人，研发投入占全年营业收入 12.83%（2024 年），绝对数额居业内前列。公司是博士后科研工作站单位，除杭州总部以外，公司还在国内、海外设立多个本地研发中心，形成了以总部为中心辐射区域的多级研发体系。

公司在中国大陆设有 32 家省级业务中心、近 300 个城市分公司和办事处，在成都、西安、石家庄等地建立科技园，在杭州桐庐、重庆、武汉等地设立制造基地；在海外，业务已覆盖全球 180 多个主要国家和地区，在 60 个国家和地区设立分支机构，并通过印度、巴西、英国等地的海外工厂实现本地化制造，为全球客户提供产品与服务。

2010 年 5 月，海康威视在深圳证券交易所上市，股票代码：002415。基于创新的管理模式，良好的经营业绩，公司荣获第五届中国质量奖[1]、国家卓越工程师团队[2]、国家科学技术进步奖二等奖[3]、2024 中国年度最佳雇主全国 20 强[4]、2023 年公司治理最佳实践案例[5]、2023 年中国企业社会责任榜责任典范奖[6]等重要荣誉。



[1] 2025 年 9 月，在中国质量（南京）大会上，第五届中国质量奖揭晓。海康威视凭借“数智质量”质量管理模式获得第五届中国质量奖。

[2] 2024 年 1 月，海康威视荣获中共中央、国务院颁发的“国家卓越工程师团队”。

[3] 2019 年 12 月、2024 年 6 月，海康威视两次荣获国务院颁发的“国家科学技术进步奖二等奖”。

[4] 2024 年，海康威视获智联招聘“2024 年中国最佳雇主全国 20 强”。

[5] 2023 年，海康威视入选中国上市公司协会“2023 年公司治理最佳实践案例”。

[6] 2023 年，海康威视荣获第一财经“2023 年中国企业社会责任榜责任典范奖”。

目 录

1 董事长寄语

“万物互联”，正在从梦想变成现实。作为“万物互联”的先行者，在过去十多年，视频监控技术发展很快，从模拟时代进入数字化时代、网络化时代，正在进入智能化时代。技术的每一次进步，在推动人类社会进步的同时，也会给人类社会带来新的挑战。互联网技术的发展，让人类社会大受其益，也给人类带来了巨大的挑战，包括网络安全的挑战。基于互联网基础上发展起来的物联网技术，同互联网一样，会让人类生活更加美好，也会让人类社会面临一些新的挑战，网络安全就是挑战之一。

相对 IT 产业，安防产业进入数字时代时间不长，安防产业界对网络安全的意识相对也弱一些。2014 年，按照惯例，海康威视成立“安全应急响应中心”，就网络安全问题建立公司统一的对外接口。2015 年，海康威视成立“网络与信息安全实验室”，网络与信息安全实验室全面推进海康威视的网络安全体系建设，先后成立网络与信息安全委员会、网络安全部，建立和完善以组织和流程为重心的网络安全体系，特别是网络安全设计，全面提升公司产品和系统的网络安全水平。

我们知道，网络安全不只是产品厂商的责任。项目的任何参与方，在项目的全生命周期，用户、集成商、运营商、工程设计方或其他服务提供商、政府，都是网络安全的责任人，都面临网络安全的挑战。三分技术，七分管理，需要所有的利益相关方共同努力迎接挑战，任何一方都不能抱有侥幸心理。

在面临行业亟需同心协力去解决这些行业所面临的共同问题的时候，我们看到公众与媒体对物联网安全表现出的极大关注与担忧，这些更让我们感受到了身上肩负的责任与使

命，海康威视将一直秉承“成就客户、价值为本、诚信务实、追求卓越”的企业价值观，我们承诺将客户的网络和业务安全性保障的责任置于公司的利益之上。

网络安全的挑战，会一直存在下去，我们会继续努力！

杭州海康威视数字技术股份有限公司

2 前言

近年来，我们见证了安防产业在数字化浪潮中的高速发展与深刻变革。人工智能技术的突破性进展，特别是 AI 大模型的产业化应用，为安防行业注入了前所未有的创新动力。同时，智能物联（AIoT）技术的深度融合使得安防系统不再局限于传统的监控功能，而是逐步演变为集感知、分析、决策于一体的综合智能平台，为实现真正的“万物互联”梦想提供了坚实支撑。

智能物联技术的广泛应用，则进一步打通了设备间的数据壁垒，推动了跨系统、跨平台的协同运作。然而，网络化与智能化在提升系统效能的同时，显著扩大了攻击面。传统封闭架构向开放网络环境的迁移，使得安防系统面临跨域攻击、数据泄露、供应链污染等多元化安全威胁。AI 大模型的引入虽增强了分析能力，但也带来了模型投毒、对抗样本攻击等新型安全风险；智能物联设备的规模化部署则增加了端点脆弱性管理复杂度。

在我们把安防从“模拟”到“数字”、从“孤立”到“网络化”、从“基础数据采集”到“智能分析”的过程中，历史遗留架构与新兴技术栈的兼容性挑战，以及快速迭代积累的技术债务，共同构成了潜在的安全风险。

海康威视作为一家全球性的公司，业务覆盖 180 多个国家和地区。面对智能化时代的机遇与风险，公司建立了覆盖研发、生产、交付、运维全生命周期的安全治理体系。我们认识到，在 AI 大模型与智能物联技术支撑下的安防系统安全，不仅关乎设备可靠性，更涉及数据主权、隐私保护与关键基础设施韧性。

网络安全并不是某个国家或公司的问题。所有的利益相关方、政府和行业都必须意识到网络安全是全球共同面临的问题，需要我们采取基于风险的方法以及最佳实践，并进行国际合作去应对这个挑战。

在此，海康威视做出了如下承诺：我们将支持和采用广义的国际认可的网络安全标准和最佳实践；我们将支持增强网络防御能力的研究工作；我们将继续改善和采用开放透明的方法，让用户能够评估海康威视的安全能力。

最后，正如我们迄今为止所做的一样，我们热烈欢迎我们的客户来帮助我们改善流程、提高技术、改进网络安全的方法，让我们可以为他们以及他们的客户带来更多的利益。

3 物联网安全威胁

物联网（Internet of Things，IoT）将任何物体通过网络相连接，给物体赋予智能，实现人与物、物与物之间的沟通和对话。海量设备的互联，使得网络更开放，也更复杂，业务更丰富多样。然而，物联网也面临着巨大的安全挑战。

图 3-1 物联网特点

物联网是由大量的设备或感知节点构成，缺少人对设备的有效监控，并且数量庞大、设备集群度高，除了传统网络安全威胁外，还存在着一些特殊安全问题。物联网的安全威胁可以根据物联网的架构分为感知层威胁、传输层威胁和应用层威胁。

感知层威胁

- 物理攻击

部署在远端的缺乏物理安全控制的物联网设备有可能被盗窃或破坏。物理接口直接暴露在设备外部，没有做安全保护，易被非法访问。

物联网设备在户外分散安装、易被接触又没有纳入管理，导致物理攻击、篡改和仿冒。

- 数据泄露

物联网设备在数据采集和处理等过程中数据未作加密或访问权限控制造成的敏感信息泄露。

- 非法接入

物联网设备缺乏有效的身份认证机制，例如使用出厂默认凭证、弱口令，或其认证协议存在可被绕过的设计缺陷。物联网设备保留了调试接口，导致攻击者可以获取设备运行信息。

- 非法更新

物联网设备的更新验证机制不健全，攻击者会将存在漏洞或包含恶意文件的非官方固件植入到设备中。

- 过期组件

物联网设备出厂时内置了存在已知漏洞的组件或过期组件，由于过期组件不再被维护，会存在极大的安全风险。

- 恶意软件

物联网设备由于性能限制缺乏安全软件防护，容易被恶意软件感染，影响设备的正常运行。

传输层威胁

- 网络攻击

网络协议本身存在缺陷如缺乏有效认证可能导致接入侧泄密。

未加密的通信过程容易发生劫持、重放、篡改和窃听等中间人攻击。

- 数据泄露

设备、云端以及移动应用端通信传输时，控制命令和采集的数据没有加密，攻击者可通过监听传输信道窃取敏感信息。

- 数据篡改

设备在网络通信时，网络传输数据没有进行完整性校验，控制命令和采集的数据可能会被攻击者篡改。

应用层威胁

- 设备管理

应用层所管理的设备分散繁多，其升级过程与安全状态难以管控。

- 越权操作

由于应用层权限管理不完善，可能存在越权问题导致重要数据被泄露。

- 系统漏洞

物联网设备的应用软件或操作系统软件存在逻辑设计的缺陷或错误，攻击者通过漏洞植入木马病毒导致设备无法正常运行。

- 数据泄露

应用层管理大量的数据，如果不做加密处理或访问权限控制容易造成数据泄露。

- 过期组件

应用层使用了包含已知漏洞的组件或过期组件，如果组件更新不及时，组件本身存在的漏洞易被利用。

- AI 模型对抗性攻击

攻击者通过向模型输入数据注入细微扰动，诱导人工智能模型输出错误决策的攻击方式。例如，对图像数据植入像素级干扰，会造成图像识别模型分类错误。

- AI 模型幻觉

人工智能模型在生成内容过程中，无中生有地输出看似逻辑自洽、实则与客观事实完全不符的虚假信息的现象。

- AI 模型虚假伪造信息滥用

利用 AI 技术生成虚假音视频内容的技术手段，其典型方式包括面部替换、语音模仿等。此类技术引发了诸如电信诈骗、人脸认证系统欺骗等安全问题。

- 配置漏洞

对应用程序、框架、容器和操作系统等执行配置时，由于配置不当导致出现安全漏洞，如使用存在安全缺陷的版本、给某些账户过高的权限、对敏感资源未做访问控制等，攻击者可非法获取重要数据。

在深入思考物联网环境中的诸多安全性隐患后，结合物联网设备在软硬件环境、计算能力等方面的复杂性，海康威视设计了以视频为核心的物联网安全解决方案，力求打造出全新的安全架构，建立多维度的安全体系，充分保障终端安全、数据安全、应用安全、网络安全、个人信息保护以及安全合规。

4 关于安防产业的网络安全

安防产业的发展历程是先模拟后数字，在模拟时代安防系统都是在专网内工作，所以产业注重的是产品的成本、性能和易用性。由于当时系统的特点，安全性一直不在考虑之中，但是随着安防产业网络化的快速推进，安防产业直接从原来的模拟进入 IP 数字化，在这个切换的过程中整个行业并未过多地考虑安全问题，这就导致了原来在模拟时代是优势、强项的易用性设计，到了数字时代可能就会与信息安全的最佳实践存在偏差。安防行业一般为了方便用户实现一键集成多个厂商设备，把所有支持的协议都默认开启，服务器端支持哪种协议就自动匹配连接，这样的设计虽然极大方便了客户，却与网络安全的最佳实践相违背。

也正是由于安防产业的这种发展历程，导致了安防产业近年来出现了一些网络安全问题，但是出现这些问题并不代表整个产业如外界所说的那么不堪一击。另外值得庆幸的是我们已经看到了这些既成与潜在的安全风险，并且已经为此开展了大量卓有成效的工作。

客观地来说，网络安全问题并不是安防产业专有的问题，网络安全是当前人类社会共同面对的一个挑战。纵观当前的整个 IT 领域，网络安全问题在所有领域都存在，并且存在以下几个基本共识：

- **安全漏洞存在的普遍性**

不存在没有安全漏洞的 IT 系统和产品，安全漏洞的存在是普遍的。由几百万行代码组成的产品，其中一个参数的设置错误，或者两行代码位置的顺序颠倒都会导致系统出现高危漏洞，目前人类的智慧还不能做到通过自动化或手动方式把所有可能的安全问题都检测出来，所以产品出现安全问题是一个正常的现象。

- **安全是整个系统的安全**

任何系统安全不是靠单点安全能够保证的，必须做到整个系统的安全。要保证视频监控系统的安全，需要系统中前端设备、后端设备、平台系统、网络设备、安全设备等相互配合、相互补充，形成纵深防御体系，才能保证整个系统的安全，任何一个环节出现问题都会导致系统被攻击。

- **第三方开源软件的安全**

当前在各种系统中会使用各种第三方开源软件，其具有开放、共享、自由等特性，在软件开发中扮演越来越重要的角色，也是软件供应链的重要组成部分，但是企业在享受开源软件带来的便利的同时，也在承担着巨大的安全风险。近年来，开源软件频繁爆出高危漏洞，例如 Struts2、OpenSSL、Fastjson 等。这些组件很多都应用于信息系统的底层，并且应用范围非常广泛，因此漏洞带来的安全危害非同一般，往往成为行业或企业产品线的“通杀”漏洞。

- **安全处于动态的平衡之中**

没有“绝对”的安全，所谓安全都是相对的，攻守的博弈永远是此消彼长。今天被认为安全的机制、方法，可能明天就是不安全的；今天被认为是“安全”的产品，可能明天就会被“攻破”。所以对于安全永远没有终点，任何一个产品在其生命周期内始终都会存在网络安全挑战和风险，只是这些风险是否会爆发以及何时爆发难以事先被预估。

- **安全地管理和使用产品**

系统安全中最重要的元素之一是管理安全。技术上再安全的系统，如果用户不能很好地管理和操作，系统的安全仍然是无法保证的，当前安防业内出现的有些安全事件的主要原因就是用户的使用“不当”，并且缺乏有效的安全管理，如目前仍然有部分安防设备在使用“弱口令”，部分安防系统在网络的边界无防火墙等安全设备。另外用户要养成良好的安全习惯，应该经常关注厂商的安全公告，有升级版本应尽快升级到最新版本。

5 海康威视安全研发成熟度模型

结合海康威视广泛的研发活动，并参考业界最佳安全实践，如 OpenSAMM、BSIMM、CSDL、MSDL 以及客户的反馈，我们制定了海康威视安全研发成熟度模型（Hikvision Security Development Maturity Model，以下简称：HSDMM），量化产品安全研发的安全活动，并通过完善的组织架构、固化的安全研发管理流程及强有力的技术手段保证安全活动的有效落地，提升产品机密性、完整性和可用性，增强个人信息保护，为客户提供更安全的产品和解决方案。后续章节我们将从安全治理、安全过程和安全技术三个维度来介绍海康威视安全研发成熟度模型。

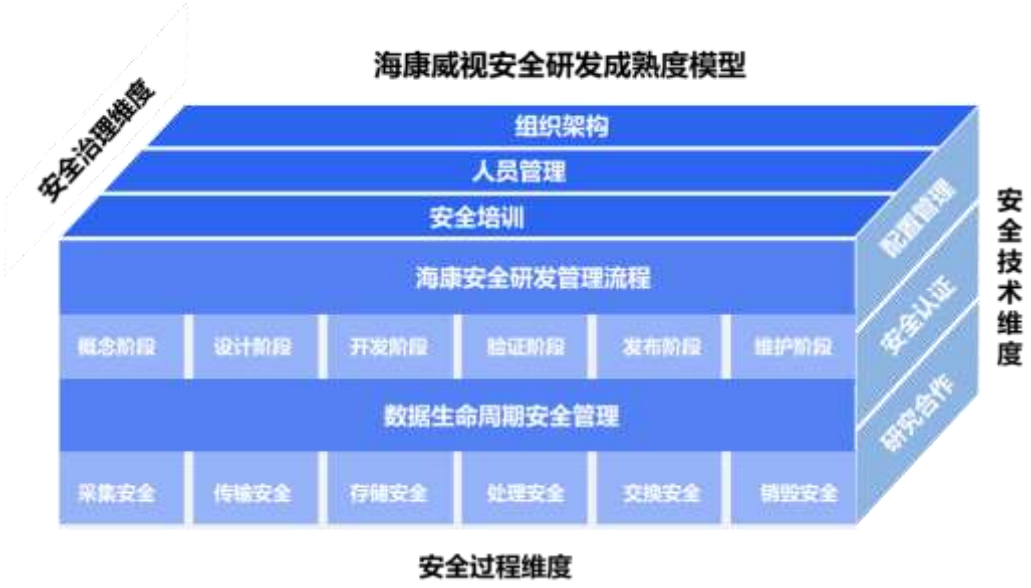


图 5-1 海康威视安全研发成熟度模型

6 安全治理

6.1 组织架构

为确保产品安全保障活动融入研发、供应链、市场与销售、工程交付及技术服务等各环节中，我们首先需要建立一个能保证其实现的组织架构，并且赋予每个组织清晰的责任。

海康威视的安全组织架构如下：

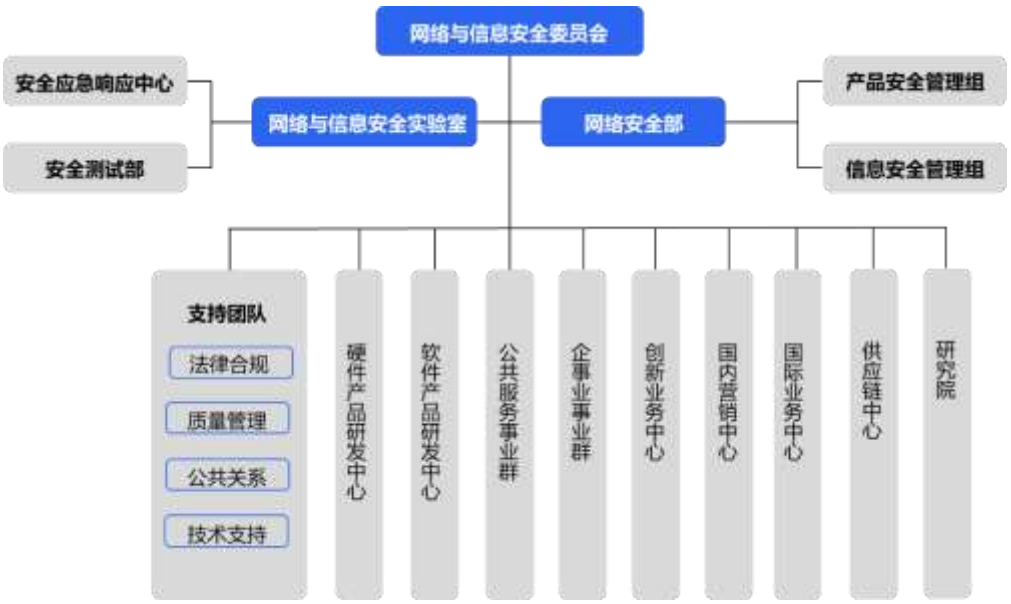


图 6-1 海康威视安全组织架构

网络与信息安全委员会

负责公司网络信息安全战略规划、政策的制定。在网络信息安全方面，如果出现了任何冲突或严重问题，该委员会有权做出决策，并对业务做出必要的调整。网络与信息安全

委员会主任由海康威视总经理担任。网络信息安全战略、政策、流程、标准的制定和资源的配置由网络与信息安全委员会常设的专门机构网络安全部负责日常管理。

网络安全部

网络安全部作为网络与信息安全委员会的常设机构，负责落实公司产品安全战略、建立公司产品安全基线、实施产品安全测评、产品安全对外合作、行业产品安全技术标准的研究和产品安全研发推进，参与产品安全的重大项目评审并为公司领导决策提供建议。结合公司产品安全战略和业界要求，建立研发安全规范，嵌入安全要素到产品研发流程，并推动在各产品线落地。

网络与信息安全实验室

网络与信息安全实验室致力于物联网相关的安全技术的研究与实践，主要覆盖物联网感知、产品安全组件、安全视频监控产品、渗透测试、物联网安全防护等多个领域，旨在研究前沿的物联网安全技术，推动物联网安全技术的进步。实验室全体人员均具备多年信息安全从业背景，其中多人拥有国家注册信息安全专业人员 CISP 或国际注册信息系统安全师 CISSP 资质证书。

安全应急响应中心

海康威视安全应急响应中心是一个负责接收、处理和公开披露海康威视产品和解决方案相关的安全漏洞平台，负责与全球范围内的其他安全组织共享安全应急的最佳实践和处置经验，增进可信沟通和合作，提升公司对安全事件应对的有效性和及时性。

产品安全管理组

海康威视各产品线均设立产品安全管理组，该管理组协同网络安全部一起建立产品安全基线及相关产品技术标准，负责相关安全要求在产品线中的产品规划、研发、测试等过程的落地实施，并对产品线的安全负责。

信息安全管理组

信息安全管理组负责协助网络安全部在公司内部推行信息安全策略、程序、规范和流程，协助完成公司内部信息安全监控、审计、培训和宣传工作，以及内部安全事件的处理。

安全测试部

安全测试部是独立于产品线的第三方部门，负责海康威视所有产品线的产品安全测试，检验公司产品安全策略、安全基线是否在产品中得到有效地执行，发现在研发过程中引入的潜在的各种安全问题，确保发布产品的安全性。

支持部门

负责提供与产品安全相关的内控、法律合规、质量运营、品牌宣传、审计及公共关系等方面的支持。

6.2 人员管理

在全员网络安全意识教育上，海康威视旨在构建全公司范围的网络安全意识教育氛围和文化氛围。为了实现此目标，海康威视对新入职的所有员工进行网络安全培训，并组织了持续的网络安全意识普及教育活动，开展基于各自业务需求的网络安全知识和技能的培训学习及其他意识教育活动，也会针对自身业务领域的特性进行网络安全案例的教育学习。公司会定期在内部宣传平台向全员开展网络安全期刊宣传，同时还会通过宣传海报、视频/微电影、开机提醒等形式向全员宣传网络安全教育内容。

海康威视对各业务领域的网络安全关键岗位进行识别，并明确定义产品安全关键岗位。对产品安全关键岗位上的员工，我们提出了以下要求：

- 员工上岗前，会通过背景调查，确保将背景和经历符合要求的人员安排到相应岗位，并签署《安全关键岗位保密协议》，明确员工的保密义务。

- 员工在岗时，会通过任职资格标准进行牵引，引导他们增强安全意识，提高相关技能，并会定期进行安全审查。

- 员工离岗时，会通过实施离岗审查要点指导人力与安全专员进行离岗权限账号的清理或修改，必要时，清理离岗员工的资产。离岗审查含内部调动离岗和离职。

我们要求每个员工都要对自己所做的事情和产生的结果负责，不仅要对技术负责，也要承担法律责任。我们的员工知道，网络安全问题一旦发生，可能会对客户、公司和个人带来极大影响。因此不管有意还是无意，海康威视都会以行为和结果为主要依据进行问责。

6.3 安全培训

海康威视参考业界优秀实践，建立了完备的网络安全培训体系。在员工入职、上岗、晋升等环节纳入多种形式的安全能力培训，提升员工的安全能力，并结合公司完善的安全研发管理流程，确保向客户提供安全、合规的产品及服务。

产品研发岗位网络安全能力认证：为加强员工的网络安全意识，提升员工的网络安全能力，提高公司产品的安全质量，针对公司从事产品软件方向的技术规划、需求设计、方案开发、编码实现、验证测试等工作的研发岗位员工进行网络安全能力认证，员工在通过网络安全能力认证后方能上岗工作或申请岗位晋升。

网络安全能力训练营：公司安全部会定期开办网络安全能力训练营，对公司的安全骨干进行集中培训，培训内容包括网络安全标准、网络安全认证、产品安全设计、威胁建模实战、产品安全问题治理等，持续提升网络安全骨干的安全能力，并更好地向各自团队赋能，最终提升所有员工的安全能力。

网络安全专项活动：公司通过开展各种实践导向的专项能力提升活动，提升网络安全关键岗位员工的知识和技能，比如：公司网络安全宣传周、网络安全专家大讲堂、网络安全案例库等。

7 安全过程

7.1 海康威视安全研发管理流程

产品的安全与个人信息保护需要依赖流程和制度进行保障，海康威视制定安全研发管理流程（Hikvision Security Development Life Cycle，以下简称：HSDLC），通过该流程把产品的安全要求与公司的研发流程深度融合，从概念、设计、开发、验证、发布、维护各个阶段都制定了明确的安全要求，确保我们产品的安全质量。

图 7-1 海康威视安全研发管理流程

概念阶段

在概念阶段，产品安全需求分析关注以下几点要求：

1. 把产品安全红线强制纳入需求列表。产品安全红线是保障安全目标实现或将风险控制在可接受水平的最基本要求，来源于法律法规、政府要求、客户准入、行业标准等，其目标是确保产品安全合规、保护用户敏感数据、加强系统访问控制、增强系统防攻击能力。

图 7-2 产品安全红线

2. 如果产品涉及个人信息，需在概念阶段识别产品涉及的个人信息数据列表。

3. 需要对该产品未来在客户现场的使用场景进行威胁分析，识别出有针对性的安全需求。威胁分析是针对产品的具体使用场景找到所有可能的威胁来源、类型以及攻击点，以便我们评估风险，确保相关的应对和防范措施纳入产品需求列表中。

设计阶段

威胁建模是在产品设计阶段执行的一项重要工作，威胁建模是一种结构化方法，利用抽象的方法来思考风险，用来识别、量化和解决与产品相关的安全风险。威胁建模的目的是在设计阶段识别系统的潜在威胁，确定风险，并建立适当的应对措施。通过威胁建模在设计阶段识别安全问题，梳理出安全需求，以便在编码阶段规避安全风险，有助于有效控制产品的安全风险并降低安全问题的修复成本。

海康威视要求所有新立项产品的基线版本必须执行威胁建模，并且安全团队会通过审计方式对威胁建模的文件进行审查：

1. 根据产品逻辑架构，通过威胁建模方法，对产品进行架构级的威胁建模，从架构层面识别产品可能受到的安全威胁，并制定对应的缓解措施。

2. 安全设计与功能设计融合，在对产品进行功能设计的同时进行功能级别的威胁建模，及时识别功能设计中的安全威胁，并制定对应的缓解措施。

3. 对收集或识别的安全需求进行详细的分析与设计，并且公司有专门的网络安全工程师在产品安全设计过程中提供专业技术支撑。

4. 对于威胁建模中遗留的高风险，进行攻击路径的分析。

5. 所有产品在设计过程中都会做攻击面最小化分析，降低产品总体的安全风险。

海康威视按照安全研发管理流程，保证产品功能设计和安全设计同步进行，可以更好地做到安全性和功能效率的平衡。海康威视基于业界通用的安全设计原则并结合公司的主要产品场景总结出关键的六项安全设计原则：攻击面最小化、最小权限、默认不信任、公开设计、默认安全和纵深防御。

图 7-3 安全设计原则

大模型技术为威胁建模提供了革命性的解决方案。通过自然语言处理与图像识别技术，大模型可自动解析设计文档中的文本和流程图信息，精准识别系统资产、数据流路径及潜在攻击面。相较于传统人工建模方式，模型能在分钟级完成对百页级文档的语义分析，结合 CWE、CAPEC 等行业漏洞知识库，自动生成包含攻击树、缓解策略及风险评级的威胁模型报告。

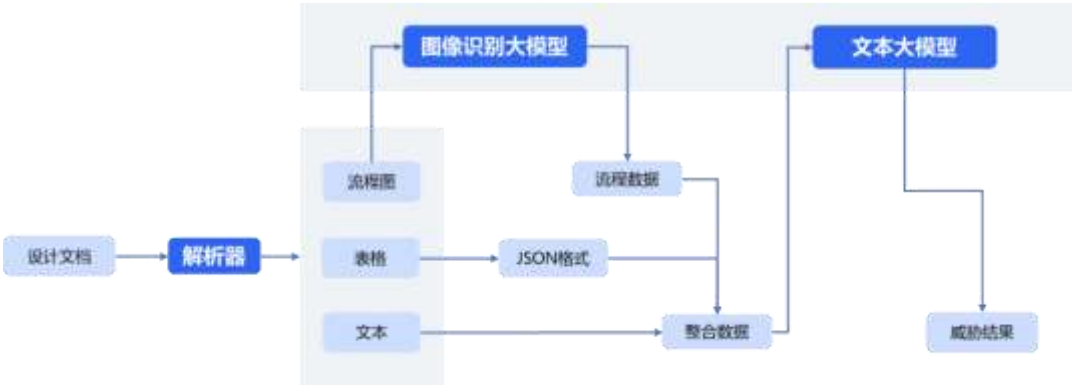


图 7-4 基于多模态大语言模型的威胁建模

开发阶段

海康威视要求研发人员在开发过程中必须遵循安全编码规范进行编码并进行交叉评审，通过自研源码扫描平台检查代码缺陷，快速、准确地查找代码中的危险函数和缺陷问题，降低代码安全缺陷率，并识别需要进一步检查的范围。自研的针对公司业务场景的代码缺陷分析和扫描工具，能够通过代码特征识别到已知缺陷，向研发通报各分支的缺陷情况，评估缺陷同步工作是否到位，并在持续构建活动中进行拦截，实现已知代码问题在源码阶段得到控制，大大降低修复成本。

大模型突破了传统工具的检测边界。基于海量开源代码训练的语义理解能力，可深度理解代码逻辑，其上下文感知特性可智能识别加密算法的弱实现、权限控制的逻辑绕过等工具难以发现的复杂缺陷，显著提升了开发团队的代码安全质量。

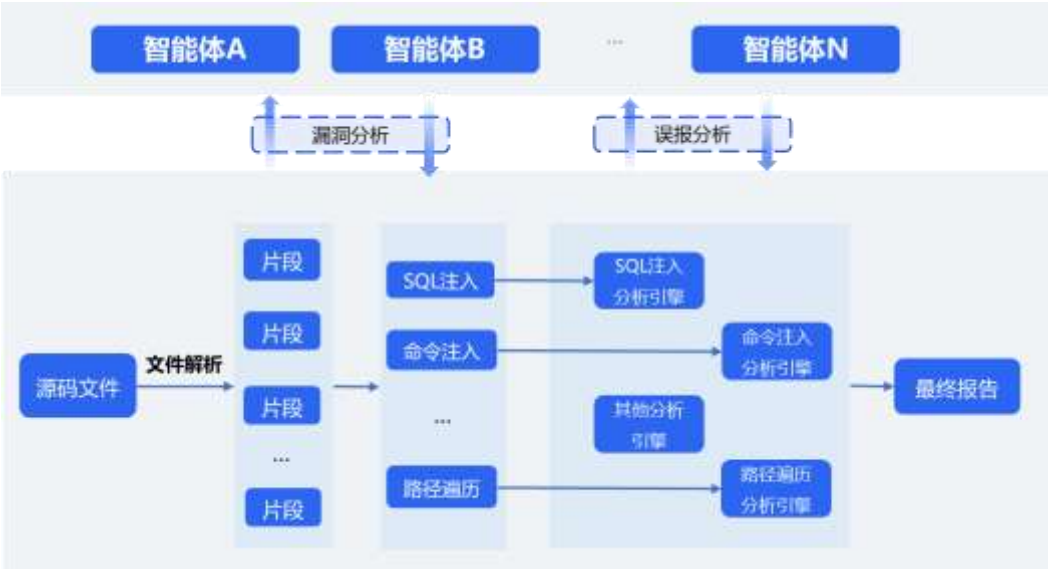


图 7-5 基于大语言模型的代码审计

验证阶段

为了保证海康威视产品的安全性，我们会在产品研发阶段进行相关的安全测试，识别研发过程中的各类安全问题，提升产品的安全性：

- 在产品安全测试中加大协议安全测试力度，对所有产品进行网络协议安全性、健壮性和可靠性测试。

- 在系统安全测试中引入漏洞扫描工具并及时更新工具所涉及的漏洞库信息，能够全面发现产品存在的各种脆弱性问题，包括安全漏洞、安全配置问题、应用系统安全漏洞。

- 在应用安全测试中引入动态应用安全测试工具，发现 Web 应用程序漏洞。

- 开展 APP 安全合规检测，满足各类安全个人信息与合规要求。

- 在产品发布前使用多款主流防病毒软件检测已知病毒、木马等恶意代码。

- 交互式应用安全测试（IAST）利用代理服务器对请求流量进行抓取和模拟测试，然后应用程序端通过配置 JVM 参数加载监控程序运行的 jar 包，可以实时监控服务端执行的所有指令，能够透明地跟踪测试脚本在内存中的流转，相对于传统黑盒测试工具，具有效率高、误报率低、告警清晰（包含调用堆栈，最终执行的命令等信息）等优点，极大地方便了开发人员对安全问题进行定位和修复。

- 公司会定期对产品进行渗透测试，最大限度地减小产品风险以保证安全风险在可控制的范围内。

- 公司产品安全管理组按季度对产品测试过程中发现的安全问题进行分析，整理出典型的安全共性问题列表，推送到各产品线进行自检，杜绝同类问题再次发生。

发布阶段

海康威视在产品发布之前，需要根据产品设计阶段制定安全测试方案与策略完成测试，测试方法包括功能性安全测试、对抗性安全测试、模糊测试、渗透测试、静态源代码审核，并通过公司自研的安全测试平台进行病毒扫描，由网络安全部和测试部进行安全性综合评估。

海康威视的产品发布包都由产品研发管理平台统一进行数字签名，保证发布包的来源和完整性，有效避免非法发布包。

维护阶段

技术支持是公司服务客户的一线人员，在获得客户授权的情况下可能会接触到客户的敏感信息。正因为如此，对他们进行必要的网络与信息安全培训非常重要，让他们可以帮助保护客户利益，防止出现访问控制问题、通信安全问题和个人信息保护问题等。在员工管理方面，公司制定了《海康威视技术支持现场服务规范》，包括行为准则、人身安全和信息安全等方面。

海康威视对可以接入客户网络的员工进行严格管理，与这些员工签订承诺书，承诺书详细说明了他们的角色、职责和潜在的法律责任，并要求他们学习网络安全知识，参加并通过相关考试。

7.2 漏洞管理

海康威视从政策、组织、流程、技术及规范等多个维度系统建设可持续、可信赖的漏洞管理体系，秉持开放协同理念，与供应链、安全研究者、监管机构等利益相关方紧密协作，共同应对安全挑战。

基于以上理念，海康威视提出漏洞管理的五项基本原则，确立漏洞全生命周期管理的五个关键阶段及相应的行为准则，全面指导各业务部门有序开展漏洞管理活动，持续提升产品与服务的安全可信水平。

安全应急响应

海康威视成立了安全应急响应中心（Hikvision Security Response Center，以下简称：HSRC），负责接收、处理和披露海康威视产品和业务相关的安全漏洞的应急响应工作，其职责还包括：

- 响应和处理客户提交的安全事件。
- 响应和处理外部机构提交的安全事件。
- 制定公司安全事件管理策略和安全事件处理方案。
- 分析软件供应链和安全机构发布的漏洞预警及安全补丁。

另外，公司还规定产品和业务相关安全事件管理的流程和各部门职责，保证产品安全事件管理的质量和效率。管理规范覆盖公司产品安全工作的售前、售中、售后全部过程，包括客户安全专题交流、安全组织合作、应急响应管理、安全公告推送、法律合规的流程和实施细则。

海康威视是国家互联网应急中心网络安全应急服务重要支撑单位，与全球范围内的其他安全组织共享安全应急的最佳实践和处置经验，增进可信沟通和合作，提升公司对安全事件应对的有效性和及时性。

图 7-6 安全应急响应

漏洞管理核心原则

漏洞管理的五大核心原则如下：

- **预防风险，守护安全**

致力于降低或消除产品及服务漏洞对客户造成的实际损害，并减少潜在的安全威胁。

- **强化防御，减少隐患**

通过提升产品与服务的防护能力，有效压缩漏洞被利用的空间。

- **主动担责，明确边界**

积极识别漏洞管理中的职责范围，梳理合规要求（如法规、合同及行业标准），并建立系统化的管理机制，实现主动管控。

- **迭代优化，追求卓越**

持续改进漏洞管理流程与规范，吸收行业先进经验，推动管理能力不断成熟。

- **开放协作，共建生态**

以开放姿态联动供应链、安全研究者、机构等各方力量，深化漏洞治理中的协同合作，构建可信的安全共同体。

漏洞处置关键阶段

海康威视参照《网络产品安全漏洞管理规定》、ISO/IEC 30111、ISO/IEC 29147等，建立产品安全漏洞处理及预警披露流程，包括 5 个阶段：

图 7-7 漏洞处理过程

➢ 漏洞研究与收集：我们通过客户、外部 CERT、安全研究人员或相关安全网站发布的资讯获取漏洞信息，同时我们通过内部团队不断发现潜在安全威胁。公司拥有完

善的漏洞披露和处理过程，并尊重每一位安全研究人员的研究结果，即外部漏洞发现者应该在公开披露之前，给厂商一段合理的时间去处理和解决问题。

- 安全漏洞评估、分析和验证：不论是疑似漏洞还是已经确认的漏洞，HSRC 团队都会与产品责任人合力快速完成漏洞的真实性及相关风险的评估。

- 跟踪与解决：一旦漏洞确认，HSRC 会立即把信息传递给漏洞提交者，然后积极跟踪反馈解决进展，并对漏洞进行排查，确保该问题在所有产品版本和产品模型中都得到解决。HSRC 流程与研发核心流程深度融合，确保对漏洞的及时响应。

在这个流程的各个阶段，保护客户和漏洞信息的机密性对海康威视来说至关重要。漏洞信息如果落入怀有恶意的人手中，会产生极为恶劣的影响，各方都必须保护其机密性。

海康威视安全应急响应团队积极参与业界与公众的活动，与 CERT、漏洞披露平台、客户 SRC、其他供应商、研究人员和第三方协调机构建立长期的联系。海康威视是国际知名漏洞信息库 Common Vulnerability & Exposures (CVE) 编号机构组织成员、国家信息安全漏洞库 CNNVD、国家信息安全漏洞共享平台 CNVD、工业和信息化部网络安全威胁和漏洞信息共享平台 NVDB 和国家工业信息安全漏洞库 CICSVD 合作单位，可以第一时间获取外部组织发现的安全漏洞，提升安全应急响应速度，为客户提供更安全的产品和解决方案。

7.3 数据生命周期安全管理

数据分类分级

海康威视制定了《信息资产安全管理程序》，依据该制度对数据进行分类分级。分类是依照数据的来源、内容和用途对数据进行分类；分级是根据数据的重要性和敏感程度以及发生数据安全事件后可能造成的危害不同对数据进行敏感级别划分。数据分为五个级别，不同级别的数据按照《数据分类分级管理规范》的要求制定不同的管理和使用策略，采取不同的保护措施进行差异化数据安全技术管控，确保技术手段和管理措施满足数据处理活动安全要求，避免敏感数据的防护不足。海康威视对个人信息等重要数据进行重点保护，对核心数据实行严格保护。

海康威视开发了公司级数据治理平台和信息资产管理系统，对全公司数据进行统一标准化管理，其中包含研发数据，对产品涉及的各类数据进行了明确定义、分类和定级，方便产品研发团队查询产品涉及数据的级别，进而拉齐全公司所有产品研发团队对于数据的定级标准和保护力度。

数据生命周期安全管理

公司的产品或服务团队应在需求分析和设计阶段考虑个人信息保护，根据具体的业务使用场景，采取适当的技术和管理措施保证个人数据的安全。如海康威视涉及处理个人信息，均在相应的产品界面中提供产品个人信息声明，描述产品涉及所有个人数据类型、目的、处理方式、留存期、风险或建议。尤其海康云端业务为用户提供个人隐私声明，说明个人信息在整个数据生命周期的安全管理措施。

个人数据主体具有知情权、访问权、纠正权、删除权（被遗忘权）、限制处理权、可携带权、拒绝权、不受自动化处理约束等权利。为了合规和更好地保护用户个人信息安全，在设计、实现产品和服务时，应纳入支持个人数据主体行使上述权利的功能。

图 7-8 数据生命周期安全管理

终端产品个人信息安全管理要求

1. 数据采集安全

按照相应法律法规要求在进行数据采集时，特别是涉及个人数据时，必须让用户知情，同时遵循用户同意、最小化采集等原则，按需采集所需数据，并且在个人信息政策中明确说明收集范围和使用目的。在用户使用海康威视 IoT 设备等涉及个人数据的服务或产品功能时，海康威视会依据所适用的法律法规，在个人信息政策中告知用户收集范围和目的，获得用户授权后按需采集个人数据。

2. 数据传输安全

在对采集数据进行传输时，对通信双方进行身份鉴别，确保接收或发送数据的实体是合法用户，此时主要使用摘要认证、数字签名等密码技术来实现身份鉴别。传输过程中通过加密、哈希、数字签名等密码技术确保传输过程中数据内容不被泄露，并保持对数据内

容篡改的及时感知。海康威视相关产品在实现数据传输安全时，使用 SSL/TLS 协议保证数据的机密性和完整性。

3. 数据存储安全

数据存储时根据数据的敏感级别进行分级隔离存储，可以使用物理隔离、逻辑隔离或虚拟化等相关技术实现不同等级数据所在区域之间的隔离。

数据存储介质可能存在无法正常工作，甚至数据丢失的情况，为了保证存储数据的可用性，需要使用冗余机制对数据进行备份，当数据存储介质重新恢复可用时对数据进行恢复还原。

数据存储后需要支持数据可溯源，根据实际业务场景使用数字水印相关技术保证数据被非法泄露后可溯源，能够追踪到泄露源头并进行相关审计。

数据存储时可使用加密、哈希、数字签名等密码技术来保证数据的机密性和完整性，保证数据被攻击者窃取的情况下也无法获取数据信息，且被非法篡改后能够被感知。

海康威视相关产品实现数据存储安全时，使用标准的密码算法对数据进行机密性和完整性保护，提供商密算法的计算模块使用符合商密规范的密码卡实现。

4. 数据处理安全

在对数据进行处理和计算时，需要保证数据的使用者具有对应的权限。使用数据时，应根据业务相关性，基于最小必要原则，对敏感数据进行脱敏处理。在对数据计算时，要保证不能从数据中间结果中得出额外的个人信息，可使用隐私计算相关技术实现数据使用过程中的个人信息保护，例如安全多方计算、同态加密、差分隐私计算等技术。海康威视

相关产品对数据处理时会对敏感数据进行数据脱敏、使用密码技术进行加密、使用隐私计算相关技术实现计算过程中的个人信息保护。

5. 数据交换安全

在数据进行交互共享时，需要对数据交换渠道进行安全管控，如强制身份验证、严格访问控制等，并采用数据水印等方式实现对数据交换过程中的数据溯源。海康威视相关产品在对数据交互时，使用密码技术保证数据的机密性、完整性和访问控制，使用数字水印技术对数据添加水印实现数据可溯源。

6. 数据销毁安全

对数据进行销毁时需要通过逻辑删除、物理销毁等方式，确保数据清除后无法被复原或再次检索到，尤其是口令、密钥等敏感数据。

云端产品个人信息安全管理要求

海康互联网业务数据存储在云端，海康云端数据安全遵守下面数据安全生命周期各阶段的数据安全保护要求。

1. 云端数据采集

明确数据采集目的、范围、来源合规。对业务数据进行数据识别、分类分级、隐私影响评估，满足数据采集最小化，获取用户知情同意，规范数据采集行为，并在个人信息政策中明确声明数据采集情况。同时，云端对采集的数据会进行合法性校验，并进行数据源鉴别及记录。

2. 云端数据传输

明确数据传输过程中通道安全、内容安全。传输层采用 SSL/TLS 协议来保证数据传输链路的安全，通过密钥管理服务（KMS）对传输数据进行加密。

3. 云端数据存储

明确数据存储加密、数字水印、审计记录、容灾机制。云端数据通过集成密钥管理服务（KMS）与硬件安全模块（HSM），实施包括字段级加密在内的多层次数据加密策略。根据业务需求也可对数据匿名化/去标识化处理，定期轮换密钥，记录审计日志，同时提供容灾机制（数据备份及恢复）。从机密性、完整性、可用性三个方面来保证数据存储安全。

4. 云端数据使用

明确数据访问控制、数据脱敏、数据水印、权限管控、审计记录要求。数据访问控制通过身份认证、权限分配、最小授权原则进行管控；对数据进行动态脱敏或静态脱敏；并进行数据水印，方便溯源；同时会记录个人敏感信息操作日志，满足合规同时监测异常。

5. 云端数据销毁

明确数据的留存期及销毁机制。根据隐私影响评估及法律法规要求确认数据的最短留存期，云端根据数据留存期进行数据销毁（物理删除、匿名化或脱敏处理）。同时用户注销后云端也会按法规要求进行用户数据销毁，满足数据销毁合规要求。

7.4 开源软件安全治理

海康威视构建了完善的开源合规管理体系，通过标准化流程、技术工具与组织保障，整合网络安全部、法律合规部、质量管理部及研发团队等资源，组建开源合规团队并制定

相应的开源安全合规管理规范。该体系深度融入安全研发管理流程，形成“事前准入预防、事中持续管理、事后应急响应”的全流程闭环管理机制，确保公司所有开源软件的安全合规性。通过该治理体系，实现安全可控、合规适配、效率协同三大核心目标：

- 安全可控：降低固件漏洞、供应链攻击及恶意组件带来的设备端与数据端风险；
- 合规适配：应对开源协议传染性、知识产权侵权等法律风险，确保组件使用与商业模式、许可证类型兼容；
- 效率协同：规范组件选型、引入与维护流程，减少重复开发与版本冲突，支撑物联网设备从研发到退市的全周期稳定运行。

图 7-9 开源软件安全合规体系

海康威视开源软件治理体系深度融入安全研发管理流程，依据公司开源软件管理规范，结合自研软件管理平台，对项目产品开发过程中的开源软件使用与发布进行全流程管控：

- 需求阶段：明确项目开源合规计划，梳理开源软件引入需求；

- 设计阶段：创建开源配置表，完成尚未引入的开源软件申请；
- 开发阶段：完善开源配置表，替换禁选软件并修复存在安全漏洞的开源组件；
- 验证阶段：对使用的开源软件进行合规与安全测试，确保符合规范；
- 发布阶段：生成并发布软件物料清单及开源许可声明文档。

8 安全技术

8.1 配置管理

配置管理是保障产品完整性、一致性、可追溯性的重要活动。通过配置管理战略和规划、配置基线管理、配置项管理、配置活动报告、配置审计、构建管理、发布管理、版本管理、组件管理和版本库管理等多个流程来保障交付的产品的完整性，并对过程中涉及的开源及第三方组件进行管理。配置管理流程是集成产品开发流程（Integrated Product Development，以下简称：IPD）不可分割的一部分，在 IPD 流程的不同阶段都开展上述配置管理活动，实现了产品的可追溯性。

构建管理规范

构建管理规范包括构建资源管理、构建过程管理、构建过程优化三个部分。配置管理中很重要的一部分就是职责分离，在构建流程规范中对构建过程中的活动、角色、职责有明确的定义。结合产品开发的不同阶段，明确构建流程在 IPD 流程中的生命周期。

编译构建中心

为了保证构建流程的可重复性和一致性，海康威视建立了编译构建中心，除了满足编译管理规范的管理要求外，还对所有的硬件、编译工具、第三方软件、数据源和操作系统做严格的准入标准控制。编译构建中心是产品编译构建的整体解决方案，提供编译构建云服务，支撑 IPD 流程中的软件构建活动。

构建过程标准化：通过工具的统一管理、构建脚本标准化、一键式构建、构建环境自动安装等，实现对产品从环境搭建、代码下载、一键式编译、打包、静态检查、自动单元测试，到系统测试整个构建过程的自动化，确保产品构建过程的可复制/还原、可追溯。

构建中心还有两个额外的功能：病毒扫描中心和数字签名中心。病毒扫描中心同时运行数十款杀毒软件进行扫描，并融入构建流程中；数字签名中心对编译的代码进行数字签名，并对签名活动进行授权和记录，确保整个工作的可追溯性。

软件与组件版本管理

海康威视借助自研的软件管理平台，完成结构化、规范化的软件版本组织结构，并着眼于软件开发整体过程，依据从需求、设计、开发、验证、发布、维护的软件生命周期管理思想，实现软件开发过程及过程数据的直观展示。

另外，海康威视使用组件化开发的模式开发产品，并以管理组件生命周期为目标，完成组件版本管理、构建管理、交付管理以及数据管理。组件在版本开发完成后，会进入组件版本验证，验证完成后，推送到软件管理平台的组件库中。组件库会标识每个组件包的名称、群组、版本、运行平台、源代码、静态分析结果、是否包含第三方软件、是否安全等信息。平台使用类似于 Maven 的方式管理 C/C++等嵌入式的组件，通过与 POM（Project Object Model 项目对象模型）逻辑一致的组件配置器集成各个组件，直至组合成一个成品软件。并依据集成的信息建立统一的版本信息结构和 SBOM（Software Bill of Material 软件物料清单）库，用于跟踪组件版本的应用情况，一旦某个组件版本出现安全问题，能快速反查使用了该组件版本的软件版本，以便维护和升级。同时能对有问题的组件版本进行禁用并提供替换版本，避免问题逃逸。

代码静态分析

在源代码的质量和安全管理中，海康威视除了采购业界优秀的商业静态检测工具外，还自研了多款针对公司业务场景的已知缺陷分析和扫描工具。

其中一款关键的自研代码特征分析工具是太鲁阁缺陷智能分析平台。太鲁阁能够基于缺陷代码特征，在全公司的代码仓库、软件版本仓库、订单系统中智能分析缺陷分布情况。系统会向研发人员通报各分支的缺陷情况、各版本的风险情况，甚至是订单的影响，保障研发能系统的评估缺陷同步工作。我们有一套完整的归零治理机制保证对太鲁阁分析识别的缺陷进行闭环。在新的代码分支产生前，我们会对源代码进行太鲁阁缺陷扫描，当存在已知缺陷时，将会提醒相关人员及时修复，若存在指定类型的高级别缺陷时，将会自动禁用该分支，要求必须先修复缺陷。在代码开发过程中，如果代码中存在已知缺陷，我们会在开发人员所使用的 IDE 中进行预警并推送相关待办催促修复。在代码开发完成并触发 CI 构建时，会触发太鲁阁的缺陷扫描功能，来检测当前分支版本是否包含太鲁阁的已知缺陷。扫描结果会即时告知构建人员，其中若存在指定类型的高级别缺陷，我们将会直接中止构建，要求必须先修复缺陷。另外，我们也增加了问题版本状态管理，在产品生命周期管理中实现软件禁用，联动生产订单系统，实现风险订单即时拦截。

另外一款自研的代码静态扫描平台支持检测空指针引用、资源泄露、缓冲区溢出等严重漏洞，支持行业编码标准检测及规则编排等能力。代码静态扫描平台兼具分析功能和管理功能，通过分析源码来识别各类问题，同时提供高效的问题管理与修复建议，并与软件管理平台集成，在软件开发阶段通过持续集成流水线来执行代码静态分析，开发人员在开发过程中就能及时关注到安全和质量，并在 HSDLC 流程中高效管理问题和解决问题，帮助研发团队全面把握并提升代码质量。

8.2 安全认证

全球法律环境错综复杂且持续变化，行业监管要求日趋严格，特别是网络安全法律领域，不少国家或地区在近些年陆续出台相关的法律法规，如中国的《网络安全法》、《数据安全法》、《个人信息保护法》，欧盟的《通用数据保护条例（General Data Protection Regulation）》、《网络与信息系统指令（NIS2 Directive）》和《网络韧性法案（Cyber Resilience Act）》等，安全合规性已然成为物联网服务提供商面临的一大挑战。海康威视致力于建立高效的安全内控体系，紧随不同行业、领域、国家的合规要求，从制度流程及控制活动等方面完善自身的合规基础。为适应全球业务拓展的需要，帮助公司在全球范围内更好地符合合规要求，推动各个国家和地区的规范经营，2018 年公司优化了内部合规组织架构，成立了合规部，负责全球合规体系的建设工作。

海康威视拥有一支内部专业律师团队对公司运营所适用的法律法规进行调查、识别和跟踪。同时，海康威视也积极与业内经验丰富的国内外知名律师事务所建立长期合作。我们建立专项工作小组，将适用的法律法规与海康威视业务实际相融合，对产品研发、制造、交付和服务各环节的法律风险进行识别和管控，提出合规建议和支持。我们持续为新入职员工、中高层管理者、网络安全关键岗位就新颁布的热点法规进行合规专项培训，不断增强合规意识。

海康威视致力于提升和完善产品的安全性，在遵从所有适用的国家和地区安全法规、参考业内最佳实践的基础上，从公司政策、组织、流程、技术和规范等方面建立和完善可持续、可信赖的安全保障体系。

海康威视支持主流国际标准，并为这些标准的制定积极做出贡献，并参与行业安全标准的制定及推广，从而进一步开放核心安全技术，与不同的行业专家和国家标准机构合作，共同完善物联网相关的安全标准体系。海康威视还与独立的第三方评估机构和人员合作，对我们的产品进行公正的安全评估和认证。

国际标准认证

海康威视通过系统性布局国际权威认证，构建了覆盖信息安全管理、隐私保护、云计算安全、漏洞治理、数据治理及工业网络安全的全方位保障体系。公司以 ISO/IEC 27001 信息安全管理体系为核心，延伸至隐私扩展标准（如 ISO/IEC 27701、29151）、云安全专项标准（如 ISO/IEC 27017/27018），并强化漏洞管理（ISO/IEC 29147/30111）。同时，通过 ISO 38505 数据治理认证，实现了从战略治理到技术落地的闭环管理。这一系列认证表明海康威视已将安全与隐私要求深度融入业务流程，持续对标国际最佳实践，为全球客户提供可信赖的产品与服务。

图 8-1 国际标准认证全景图

ISO/IEC 27001

ISO/IEC 27001 信息安全管理体系是国际上针对信息安全领域最权威、严格，也是最被广泛接受及应用的体系认证标准。通过该认证，就意味着企业已经建立了一套科学有效的信息安全管理体系，以统一企业发展战略与信息安全管理的步伐，确保相应的信息安全风险受到适当的控制与正确应对。海康威视自 2012 年首次建立信息安全管理体系，经过近十年的持续革新与完善，于 2021 年正式发布海康威视信息安全管理体系 3.0，该体系覆盖了包括网络安全、信息安全和隐私保护的管理要求，遵循 PDCA 持续改进的方针，为海康威视的业务提供了可靠的支撑和保障。

2023 年 1 月，海康威视通过国际权威审核机构——英国标准协会（BSI）的认证，成为全球首批获得 ISO/IEC 27001:2022 认证证书的企业，标志着海康威视信息安全管理能力已处于国际领先的行列。

ISO/IEC 27701

ISO/IEC 27701 是信息安全管理标准 ISO/IEC 27001 的隐私扩展，用于帮助组织有效保护和合规处理个人信息。该标准是目前全球最具权威的隐私保护标准，是国际公认的隐私保护最佳实践的指南，同时也为 GDPR 中提及的“适当的技术和组织措施”提供指导意见，成为隐私相关法律合规的重要参考和支撑依据。

海康威视于 2021 年 12 月获得由 BSI 颁发的 ISO/IEC 27701:2019 认证。

ISO/IEC 29151

ISO/IEC 29151 标准针对全球 IT 技术高速发展中的个人信息安全面临的安全问题，以保护个人信息为核心，规范个人信息收集、存储、处理、使用和披露等各个环节中数据操作的相关行为，进一步加强对个人可识别身份信息风险，进行准确评估并采取有效的控制措施，提高业务流程的安全性和可靠性，降低 IT 运营过程中的个人可识别身份信息风险，最大程度地保障用户合法权益和社会公共利益。

海康威视于 2021 年 12 月获得由 BSI 颁发的 ISO/IEC 29151:2017 认证。

ISO/IEC 27017

ISO/IEC 27017 是在 ISO/IEC 27002 基础上面向云计算场景的安全控制实践指南，为云服务提供方和云服务使用方分别给出了额外的控制项和实施指引，明确共享责任边界，聚焦虚拟化资源管理、云管理员权限、安全日志、跨租户隔离等云特有风险。该标准帮助组织在构建或使用云服务时，将信息安全管理体系从传统 IDC 延伸到云环境。

海康威视于 2024 年 12 月获得由 BSI 颁发的 ISO/IEC 27017:2015 认证。

ISO/IEC 27018

ISO/IEC 27018 是专门面向公有云环境中个人可识别信息（PII）保护的隐私扩展标准，以 ISO/IEC 29100 隐私框架为基础，结合 ISO/IEC 27002 的控制原则，为作为 PII 处理者的公有云服务提供方制定了通用控制目标和实施措施，涵盖数据收集、使用、存

储、删除以及审计、透明度和合同条款等要求，帮助云服务满足 GDPR 等隐私法规要求。

海康威视于 2024 年 12 月获得由 BSI 颁发的 ISO/IEC 27018:2019 认证。

ISO/IEC 29147

ISO/IEC 29147 是国际上针对安全漏洞管理的核心标准：聚焦漏洞披露，指导厂商如何建立规范的漏洞接收、沟通与公开机制。该标准与 ISO/IEC 30111 标准相互补充，构成了覆盖“发现—披露—修复—通报”全链条的漏洞管理体系，有助于提升组织应对安全漏洞的透明度、及时性和可追溯性，增强与客户、伙伴及安全社区之间的信任。

ISO/IEC 30111

ISO/IEC 30111 是国际上针对安全漏洞管理的核心标准：聚焦漏洞处理，规定从漏洞受理、验证分析，到修复发布、风险通告的全流程管理要求。

海康威视于 2025 年 12 月获得由 BSI 颁发的 ISO/IEC 29147 与 ISO/IEC 30111 认证，标志着公司在产品安全漏洞管理和协同披露方面已全面对标国际最佳实践。

ISO 38505

ISO 38505 是数据治理领域的重要国际标准，用于指导组织在数据全生命周期中实现有效、合规和可审计的治理决策。该标准将数据治理纳入整体公司治理与 IT 治理框架之中，强调在数据质量、数据安全、数据资产价值挖掘之间取得平衡，通过明确治理主体、决策原则和责任边界，帮助组织在支持业务创新的同时降低数据相关的合规与运营风险。

海康威视于 2023 年 12 月获得由 BSI 颁发的 ISO 38505-1:2017 认证，并持续保持及拓展认证覆盖范围，将数据治理要求全面融入公司数据管理与安全管理实践。

ISO 28000

供应链系统具有参与主体复杂多样、过程环节步骤众多、产品传递跨地域等特征，这使供应链系统容易受到来自内部的不利因素的影响和来自外部的威胁。供应链系统面临的安全威胁主要包括未经授权的生产、篡改、盗窃、植入恶意软件及硬件，以及供应链中不良的制造和开发实践。供应链系统的漏洞可能潜伏数年才被发现，而且在很多情况下，难以确定安全事件是否是供应链漏洞的直接结果。供应链的安全问题有可能对组织造成持续的负面影响。

为了解决制造安全风险，确保硬件和软件的完整性，海康威视在产品生产关键环节，包括软件提供、芯片烧录/校验、软件加载、生产测试等，采取防篡改、防植入、防调包等安全管控措施，以防范未授权的硬件替换、软件植入或篡改、病毒感染等风险。产品数据管理系统把设备需要烧录的软件下载到一个安全的制造分发系统，软件在烧录之前会经过多次完整性验证。

供应链用于生产的软件烧录、软件加载、组装和测试网络隔离于公司的办公 IT 系统和公共互联网之外。

海康威视不仅通过技术手段来提高供应链的安全性，还通过管理体系建设来保障供应链的安全。ISO 28000 供应链安全管理体系的目标是全面改进供应链的安全，它能帮助组织各部门审核安全风险并实施控制和减轻风险的措施来应对供应链潜在的安全威胁。ISO

28000 与 ISO 9001 质量管理体系及 ISO14001 环境管理体系是兼容的，可以在一个组织内把质量系统、环境系统和供应链安全管理系统整合起来。

海康威视在明确供应链运作环境、识别各个环节威胁并进行风险评估和应对的基础上，建立了一个全面符合 ISO 28000 的供应链安全管理体系，并且通过 PDCA 管理循环，实现供应链安全管理体系的不断更新和完善。

海康威视实施了一个安全、严格的维护流程，确保流程中产品的完整性。公司在制造和条码系统中记录整个流程中的信息，为研发、采购、生产制造（芯片烧录、软件加载、组装、测试等）、仓储、物流环节建立详细的执行记录及日志，以确保可追溯性。

国际通用标准认证

海康威视已构建覆盖信息安全、软件开发与数据合规的国际化标准与实践体系。该体系不仅包含 CMMI5 级软件成熟度认证、IEC 62443-4-1 工业网络安全开发生命周期认证等国际权威认证，还通过将 Privacy by Design 原则深度融入研发流程、建立完善的漏洞管理机制等系统性实践，以持续满足 GDPR 与欧盟《网络韧性法案》（CRA）要求，确保产品全生命周期的安全性与合规性。

IEC 62443-4-1

IEC 62443-4-1 是 ISA/IEC 62443 工业网络安全系列标准中面向产品供应商的安全开发生命周期（SDLC）要求，覆盖安全管理、安全需求规范、架构设计、安全实施（含安全编码）、验证与确认、缺陷管理、安全更新管理、安全指南八个实践领域，强调将安全嵌

入工业及嵌入式产品从立项到退市的全生命周期过程，提升产品在工业自动化与控制系统（IACS）环境中的抗攻击能力和可维护性。

海康威视于 2025 年 1 月获得 IEC 62443-4-1 安全开发生命周期认证。

CMMI5 软件成熟度认证

CMMI 即能力成熟度模型集成，是企业级过程管理的框架，是世界最优秀企业的最佳实践，是业界公认的衡量企业产品及服务能力的权威标准，同时也是过程改进的方法，可以帮助企业实现商业目标、确保质量、保证交付、提高客户满意度。软件 CMMI 规范中针对企业改进过程能力设定了 5 个阶梯式上升的成熟等级，其中 5 级为最高级别。

海康威视于 2016 年 4 月成功通过 CMMI5 认证。

CSA-STAR 认证

CSA-STAR 认证是一项有针对性的国际专业认证项目，由全球标准奠基者——英国标准协会（BSI）和国际云安全权威组织——云安全联盟（CSA）联合推出，旨在应对云安全相关的特定问题。

云安全国际认证（CSA-STAR）以 ISO/IEC 27001 认证为基础，结合云端安全控制矩阵 CCM 的要求，运用 BSI 提供的成熟度模型和评估方法，为提供和使用云计算的任何组织，从沟通和利益相关者的参与、策略、计划、流程和系统性方法、技术和能力、所有权、领导力和管理、监督和测量等 5 个维度，综合评估组织云端安全管理和技术能力，最终给出独立第三方外审结论。

海康威视于 2021 年 12 月成功通过 CSA-STAR 认证。

ETSI EN 303 645 消费类物联网安全标准

ETSI EN 303 645《消费类物联网网络安全：基线要求》是由欧洲电信标准化协会（ETSI）发布的首个面向消费类物联网设备的全球通用网络安全标准。该标准围绕“禁止通用默认密码、提供漏洞披露通道、保持软件持续更新、保护敏感安全参数、加固通信与攻击面、保障个人数据安全”等 13 个安全类别提出 30 余项强制要求和若干建议，覆盖智能摄像机、家用路由器、门锁、智能家电等各类联网终端，为英国 PSTI、新加坡 CLS、IECEE CB 等多国法规与认证方案提供了统一的技术依据。

随着 EN 303 645 被纳入 IECEE CB 体系的 CYBR 类别，多家国际权威检测机构可基于该标准出具 CB 型式试验报告和 CB 证书，用作全球多国准入与本地认证的“通行凭证”。

海康威视积极对标 EN 303 645 的安全要求，对前端摄像机、后端 NVR 及云平台管理软件进行系统性安全加固和测试。截至 2025 年，海康威视多款前端网络摄像机系列、后端 NVR 产品系列以及 HCP 软件平台，已通过多家国际检测实验室依据 EN 303 645 开展的网络安全测试，获得相应的 CB 证书，表明相关产品在身份认证、安全配置、固件更新、漏洞处理、数据传输与隐私保护等方面符合国际主流消费物联网安全基线要求，为全球用户提供了更高水平的安全与可信保障。

通用数据保护条例 GDPR

海康威视致力于保护个人数据并全力支持 GDPR 要求的实施。海康威视一直采取多项举措来保护个人数据，包括通过数据收集授权、最小化数据收集、数据匿名化、通信和存储加密、数据安全审计等。为了确保产品和服务在设计之初即兼顾隐私保护，公司在内部推广 Privacy by Design（PbD）原则，在需求分析、架构设计、测试发布等各阶段嵌入隐私评估要求，并针对涉及大规模或高风险数据处理的业务开展数据保护影响评估（DPIA），识别并降低潜在隐私风险。公司制定并实施了一系列数据保护政策，建立数据保护工作组，将 GDPR 要求融入海康威视的业务运营、合同管理和供应链管理中，持续强化对用户个人数据的保护能力。

网络韧性法案 CRA

面对欧盟《网络韧性法案》（Cyber Resilience Act, CRA）对“具有数字元素的产品”在本质安全、漏洞管理和强制上报方面提出的系统性要求，海康威视从产品全生命周期角度规划应对举措。一方面，公司强化安全开发流程，将安全需求分析、威胁建模、安全编码规范、SBOM 管理和安全测试纳入标准研发流程，逐步对齐 IEC 62443-4-1 等安全开发标准；另一方面，围绕漏洞管理和事件响应，依托内部漏洞管理机制，规范漏洞受理、分级评估、补丁发布和客户通报流程。

各国标准合规

海康威视持续完善全球化的信息安全与合规体系，在国内外标准及法规方面取得显著成果：在国内通过信息安全等级保护三级测评，确保关键信息系统的安全建设符合国家标

准；在国际层面，基于 NIST CSF 2.0 框架系统化提升网络安全治理与风险管理能力，并积极应对英国 PSTI 法案、巴西 Anatel 网络安全要求等区域法规，通过取消默认密码、强化漏洞管理、固件更新机制等措施，实现产品在多个市场的合规准入，形成覆盖全球的安全与隐私保护能力。

信息安全等级保护认证

信息安全等级保护是我国信息安全保障的一项基本制度，是保护信息化发展，维护国家信息安全的根本保障。信息系统的安全保护等级是根据信息系统在国家安全、经济建设、社会生活中的重要程度，以及遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素将其划分为五个等级，五级为最高系统等级。

依据《信息安全等级保护管理办法》的有关规定，萤石云、海康威视内部信息系统已通过信息安全等级保护三级测评，严格遵循国家在信息系统安全建设方面的技术保障和安全管理要求，建立了自身的长效机制，进一步保证安全保护工作的持续进行。

NIST CSF 2.0

NIST 网络安全框架（Cybersecurity Framework，CSF）由美国国家标准与技术研究院发布，是面向各类组织的网络安全风险管理框架。2.0 版于 2024 年正式发布，在原有“识别 - 保护 - 检测 - 响应 - 恢复”基础上新增“治理（Govern）”职能域，进一步强化高层治理、供应链安全与度量改进，并通过实施示例和参考映射帮助组织评估、规划和持续提升网络安全能力。

海康威视于 2025 年 7 月通过基于 NIST CSF 2.0 的第三方评估认证，系统验证公司网络安全治理与风险管理能力。

8.3 安全技术

网络与信息安全实验室致力于物联网相关的安全研究与实践，工作内容包括渗透测试、模糊测试、代码审计、逆向分析、漏洞研究、工具开发、物联网安全方案分析与研究。团队主要研究方向覆盖 WEB 安全、移动安全、协议安全、无线安全、固件安全、威胁情报、机器学习等多个领域，旨在先于黑客发现并及时解决安全问题。

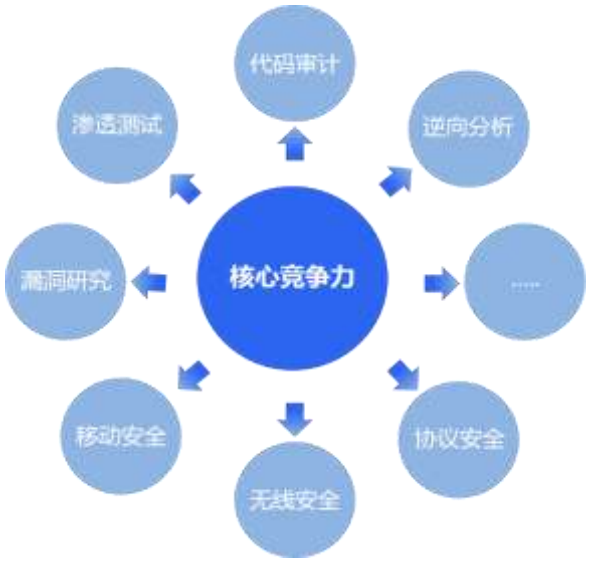


图 8-2 产品安全核心竞争力研究

核心竞争力：

- 嵌入式设备漏洞挖掘：结合海康威视在嵌入式设备安全领域的经验，使用固件逆向、固件仿真、串口调试、静态分析、符号执行等手段进行漏洞挖掘。

- 协议漏洞挖掘：集成商业工具和自研模糊测试工具，利用 Fuzzing 技术对主流物联网设备协议进行自动化漏洞挖掘，目前已发现数百个协议高危漏洞。

- 无线安全研究：团队拥有 RFID、无线射频、蓝牙模块等多种安全硬件测试环境，可实现无线数据报文窃听、无线信号重放攻击、无线信号欺骗攻击、无线信号劫持攻击、RFID 破解攻击、NFC 克隆攻击。

- 白盒审计：集成商业工具对所有内部使用的开源组件已知漏洞进行跟踪检测、威胁预警；内部团队在渗透测试过程中将针对目标源码进行白盒审计，全面提升漏洞挖掘效率。

- Web 安全：集成商业工具和自研 Web 测试工具，利用爬虫探测技术和被动代理技术对 Web 平台进行渗透测试，支持对 SQL 注入、XSS 跨站脚本、敏感信息泄露、命令注入等各类 Web 安全问题的检测，核心安全测试团队将对目标系统进行深入的渗透测试以发现更多潜在安全漏洞。

- 移动安全：团队结合内部移动安全检测分析工具，对移动 APP 进行全方位的安全检测，支持实时捕获交互协议报文、敏感信息自动识别；支持移动 APP 个人信息合规检测；支持对移动 APP 进行安全加固，防止恶意攻击。

- 威胁情报：团队搭建多种类型分布式高/低交互蜜罐，可全网实时感知各种物联网恶意攻击及攻击样本捕获并进行实时关联分析预警。

- 机器学习：团队利用机器学习算法对物联网设备日志进行安全分析，提供多种安全攻击检测模型，可以快速从海量日志中发现潜在或已知的恶意攻击行为并进行实时威胁预警。

安全引擎

物联网安全防护引擎

为不断提升物联网设备对网络攻击威胁的检测和防御能力，网络与信息安全实验室团队自研开发了可应用于物联网设备中的入侵防御、协议防火墙等安全检测防护引擎。实现对物联网设备的状态全程监控、风险全面感知、攻击实时阻断的安全防护能力。并支持通过热更新的方式不断进行无损升级以应对日益变化的新型网络攻击，为物联网设备稳定可靠运行保驾护航。

入侵防御引擎

入侵防御引擎专门为公司物联网设备进行设计开发，物联网设备内置入侵防御引擎模块，实现开机后全程对设备的文件、网络、进程等状态和操作行为进行实时的监控和分析，通过进程白名单的方式阻断恶意进程的启动和运行；对恶意文件的创建、删除、修改等操作进行全程监控和检测拦截，并对非正常的设备外联网络行为进行实时监控和阻断。

协议防火墙引擎

物联网设备由于资源限制无法应对大规模的恶意扫描及网络攻击，常规的安全防护软件无法进行部署使用。为有效抵御常见的网络攻击对设备安全稳定运行的影响，公司安全团队开发轻量级物联网协议防火墙引擎模块，对原始的请求报文内容在进入业务处理逻辑

之前，进行网络攻击行为检测，发现攻击行为后及时阻断报文，并根据拦截策略决定是否对攻击目标进行自动封禁。通过与业务模块的深度集成突破了传统安全防护产品无法对加密报文进行安全检测的痛点，并可对各种物联网协议进行全面的检测和深度分析，可有效抵御各类常见的网络攻击，提升物联网设备的安全稳定运行能力。

安全态势感知

由终端与设备、通信与网络、平台与应用构成的庞大的物联网系统，不但需要具备每个层面的多重安全防护，还需要具备“端云协同”的智能大数据安全分析能力。实现整网的智能安全态势感知、可视化和安全防护，必将是物联网安全的发展方向。

安全态势感知是在大规模系统环境中，对能够引起系统状态发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。

图 8-3 安全态势感知

脆弱性评估

脆弱性评估是决定安全态势感知系统能否有效检查安全隐患的关键。海康威视安全态势感知系统集成业内主流的漏洞库，可针对目前已知的漏洞进行检查。另外，海康威视拥有专业的漏洞研究团队，不断跟踪其他知名安全组织和厂商发布的安全公告，并持续分析、挖掘、验证各种新型漏洞。借助海康威视专业漏洞研究团队的持续投入和漏洞库的持续升级，可及时帮助用户发现安全隐患，防患于未然。

除此之外，海康威视安全态势感知系统还可对发现的安全威胁和资产信息进行关联分析，通过建立的大数据分析模型对实时数据和历史数据进行动态分析，可准确、高效地感知整个网络的安全状态以及发展趋势，从而对智能物联系统进行安全加固，保障系统安全。

安全可视化

可视化展示能够直观地呈现数据特点，同时容易被使用者接受和理解，所以大数据分析（深度包检测、全流量分析）结果需要可视化展示。

当系统遭到攻击时，需要快速地识别攻击来源和攻击路径，对攻击做出快速地响应，在攻击造成更大的破坏之前，实施有效的措施，减少损失。在攻击之后，需要快速地防止此类攻击的再次发生。

安全中心

作为系统安全防护的核心组成部分，安全中心旨在通过智能化检测与可视化监控，帮助用户构建坚固的安全防线。主要包括以下三大模块：账户安全、配置安全和基础安全。

账户安全：涵盖用户管理、密码重置预留信息、登录管理等方面不安全配置及异常操作行为的风险提示。

基础安全：涵盖可信保护、固件加密、配置文件安全、安全备份、存储加密、安全防御、安全审计等子项，确保系统基础环境稳固。

配置安全：通过检测常见服务配置，对用户启用的不安全协议进行风险提示，以保障使用安全。

图 8-4 安全中心示意图

蜜罐

蜜罐技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网

络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机。

得益于数据存储、数据检索、数据挖掘和威胁情报等技术的兴起和发展，蜜罐技术的价值可以被更充分地发挥。海康威视基于自研和改造的蜜罐作为数据采集器，在全球范围内部署蜜罐节点，并建立了对蜜罐数据进行收集、处理、存储和检索的蜜罐数据管道，为安全研究、应急响应、攻击溯源和态势感知提供数据支撑。

海康威视蜜罐系统基于规则引擎，实时监测针对物联网设备的攻击行为，并对未知威胁进行预警。蜜罐系统的分析引擎基于蜜罐系统的历史数据，可以对恶意攻击者进行重点监控和关联分析，并预测威胁趋势。

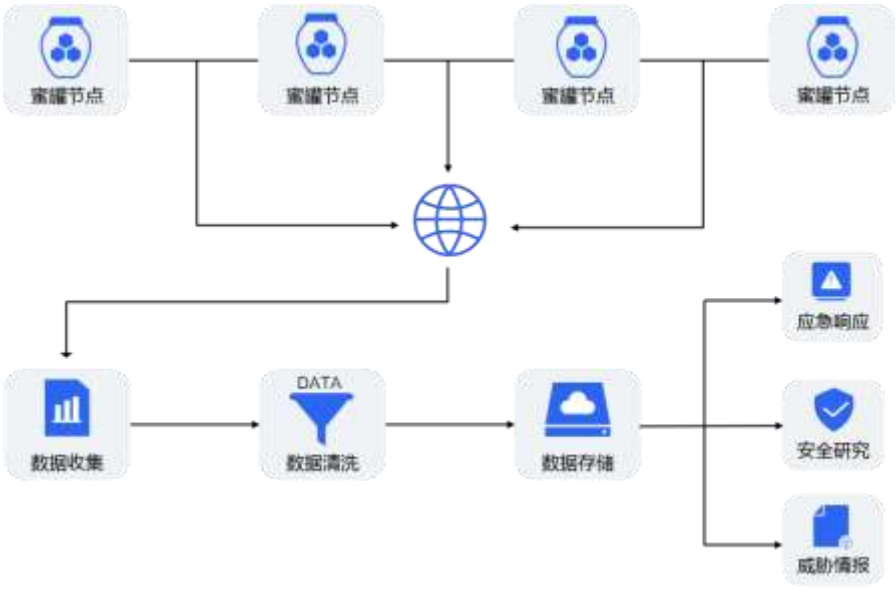


图 8-5 蜜罐系统

海康威视的蜜罐系统作为海康威胁情报平台的重要组成部分，将持续监控来自全球的安全威胁，保障用户设备的安全稳定运行。

数字水印

数字水印是将标识信息嵌入数字载体（图像、音频、视频、文档等）中，在不影响载体正常使用的前提下，实现版权确认、内容认证或隐蔽通信的技术。其核心原理基于信号处理与密码学，通过修改数据比特或引入不可察觉的冗余信息隐藏水印，同时保证水印的可检测性与安全性。

进一步，模型水印是面向AI模型（尤其是生成式模型）的水印技术，通过在模型参数、训练过程或生成内容中嵌入标识信息，实现模型所有权验证、生成内容溯源与知识产权保护的技术。

数据水印是抵抗数据泄露的“最后一道防线”。因此从水印技术本身来说，它具有广泛的应用前景和巨大的经济价值。

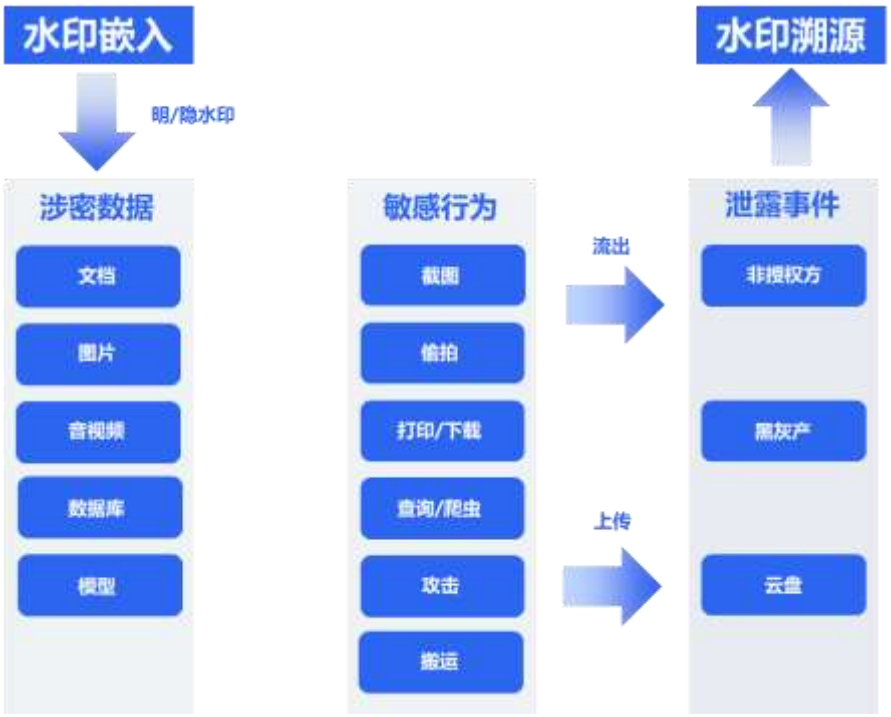


图 8-6 数字水印

随着《人工智能生成合成内容标识办法》以及配套的强制性国家标准《网络安全技术 人工智能生成合成内容标识方法》同时出台，数字水印与模型水印技术的应用将更加广泛且重要。海康威视是国家标准《GB/T 45909-2025 网络安全技术 数字水印技术实现指南》的核心参编单位之一，在安全鲁棒的多模态隐式水印/显式水印、模型水印上具备丰富的技术储备。

9 人工智能安全

随着人工智能（Artificial Intelligence，AI）技术的规模化应用，其已渗透至个人生活（如智能家居、智能门禁）与公共服务（如智慧交通系统、城市公共安全治理）等多个领域。AI 安全是保障此类智能应用合规、可靠运行的核心前提，直接关系到个人隐私权益、企业财产安全及社会公共利益。

AI 安全是人工智能技术与信息安全的交叉领域，聚焦于两大核心目标：一是保障 AI 系统自身的安全、稳定与可靠运行，使其具备抵御各类攻击的能力；二是防范 AI 技术被恶意滥用，以规避其对个人、企业及社会造成的潜在危害。

近年来，生成式人工智能（含智能对话助手、图像生成工具）、大模型等技术快速演进，显著提升了 AI 的应用能力，但也加剧了安全风险的复杂性与扩散性。大模型凭借跨领域理解与生成能力赋能生产生活的同时，其复杂的模型结构、海量的训练数据及开放的交互模式，催生了提示注入、模型越狱、生成内容滥用等新型安全风险。例如，不法分子利用大模型技术批量生成虚假信息、优化欺诈手段，不仅提高了攻击的精准性与效率，也大幅增加了安全防护的难度与挑战。

为规范 AI 技术发展、防范安全风险，全球多个国家和地区已出台针对性政策法规。

国内方面，我国已建立起多层次、系统化的 AI 安全治理体系。2026 年 1 月 1 日施行的《中华人民共和国网络安全法》新规，首次将人工智能纳入国家网络安全法律体系，明确支持 AI 基础研究与基础设施建设，要求完善伦理规范和风险监测评估机制。《生成式人工智能服务管理暂行办法》自 2023 年 8 月 15 日起正式施行，对生成式人工智能服务实行包容审慎和分类分级监管，明确了提供和使用生成式人工智能服务总体要求。《人工智能生成合成内容标识办法》于 2025 年 9 月 1 日起施行，并配套推出强制性国家标准。该办法和相

关标准聚焦人工智能“生成合成内容标识”关键点，通过标识提醒用户辨别虚假信息，明确相关服务主体的标识责任义务，规范内容制作、传播各环节标识行为。

国际方面，欧盟《人工智能法案》作为全球首部综合性 AI 监管法规，已于 2024 年正式生效。该法案基于人工智能系统对用户和社会的潜在影响程度，将人工智能风险分为禁止、高风险、有限风险和最低风险 4 个级别，并据此设定不同的监管要求和合规标准。

9.1 AI 模型安全评测

随着边缘终端计算资源的提升，海量边缘终端通过内置的人工智能算法和硬件支持，实现了语音识别、图像处理、自然语言理解、预测分析等功能，从而提升了用户体验和设备性能。然而，边缘终端智能算法模型应用日益广泛、规模日趋庞大、结构愈发复杂等特点，导致其面临数据、模型、算法等多个层面的安全威胁，例如对抗性样本攻击、训练数据毒化攻击、模型后门植入攻击等。此类问题不仅直接威胁到模型的安全使用与运行效能，还可能侵犯数据隐私，导致系统整体功能失效。

针对以上问题，海康威视深入研究了智能模型高效安全评测、安全风险实时监测等技术，构建了人工智能算法模型安全评测平台，覆盖主流人工智能算法模型，支持鲁棒性、公平性、可解释性等多维度评测，满足万亿参数级智能模型的脆弱性检测与主动风险防控需求。

具体而言，平台针对物联网智能模型种类多、更新迭代快、数量规模大，应用场景多等特点带来的异常样本少、黑盒测试难度大、测试覆盖率不足的问题，构建了动态可编排的大规模智能模型脆弱性扫描框架，依托测试样本自动生成、对抗样本测试、隐私泄露检测、模型后门扫描等关键技术，精准识别对抗攻击、数据投毒、模型窃取等典型安全风险。平台面向真实智能物联网场景，提供一键式、多类型的黑盒智能安全自动测试能力，可自定义测试

配置，并提供测试报告自动化生成功能，实现可视化、可验证、高效率、系统化的智能算法模型安全评测。

此外，海康威视面向大语言模型以及多模态大模型，构建超百万条的大模型安全评测数据集，配套涵盖生成内容合规、拒答能力、幻觉输出、信息安全等十余大类专项安全能力评测，实现大模型安全风险的有效排查。

9.2 AI 安全防护增强

模型防护增强

模型安全是AI安全的核心环节，核心防护技术包括对抗训练、模型加密、数据预处理等。

对抗训练通过在模型训练过程中主动引入对抗样本（指施加微小扰动的输入数据），提升模型对恶意扰动的抵御能力，降低对抗性攻击的影响。

模型加密技术通过对训练完成的模型参数与结构实施加密处理，部署时通过安全硬件（如TPM/TEE可信执行环境）解密运行，防止参数被非法提取，保护企业核心AI资产。

数据预处理技术通过对输入数据进行滤波、归一化、去噪处理，消除对抗性扰动的影响，从而有效抵御攻击。

权限与部署环境防护技术包括：

1. 严格划分模型训练、部署、推理阶段中的用户权限，例如仅允许管理员修改模型参数，普通用户仅能调用推理接口，避免权限滥用；

2. 采用沙箱或容器化部署，隔离模型与主机系统的资源，防止模型被恶意程序攻击或篡改；

3. 定期对部署环境进行漏洞扫描与补丁更新，包括操作系统、深度学习框架、依赖库的安全加固；

4. 记录全链路操作审计日志，包括用户身份、操作时间、请求内容、模型输出，实现安全事件的追溯与分析。

数据安全保护

数据是AI模型训练与推理的核心基础，数据安全是AI安全的前置条件。海康威视围绕数据加密、数据隐私保护、数据泄露检测等维度提供AI数据全生命周期安全保护。

数据加密技术主要解决数据在静态存储、动态传输等过程中的安全问题，包括：1）使用加密算法对原始训练集和模型权重进行加密；2）使用安全传输协议、数据完整性保护等手段保护数据传输安全。

数据脱敏作为一种关键的隐私增强技术，通过对敏感个人信息进行泛化、抑制、扰乱或加密等处理，确保数据在训练与使用过程中不泄露原始个人信息。

数据泄露检测技术侧重于识别未经授权的数据外传或模型异常行为，不仅需检测原始数据的直接泄露，还需检测通过模型输出、参数、梯度等间接泄露的风险。

10 交流合作

海康威视通过对外交流与合作，接纳利益相关方的反馈，吸收安全领域先进技术和管理经验，系统地转化为未来改进的目标，不断提升公司的信息安全能力。

图 10-1 交流合作

- 邀请国内外知名安全评估机构对公司的研发安全管理体系进行对标建设，保证海康研发安全体系与国际一流公司看齐。

- 加强与国内外安全厂商的交流与合作，提升公司产品的安全性。

- 邀请国内外知名的安全测试团队对公司产品进行渗透测试，最大限度地减小业务风险以保持安全风险在可控制的范围内。

- 邀请国内外知名安全专家来公司授课，提高员工的安全业务水平。

- 公司每年均与客户进行多次有关产品安全专题、应急响应工作机制和安全需求的交流，并及时向客户推送安全进展，了解客户需求。

- 公司面向社会推出的“安全白帽子奖励计划”对关注海康威视信息安全的国内外白帽子进行奖励，回馈推进海康威视产品安全不断进步的优秀安全技术研究者。

11 安全性承诺

海康威视致力于使用领先的安全及个人信息保护技术来帮助客户保护其个人信息，以及采用全面的方法来保护用户的数据。

海康威视在整个视频物联网应用生态系统中使用统一的集成安全基础架构。海康威视拥有一支专业的安全团队，负责为所有海康威视产品提供支持。该团队为开发中和已发布的产品提供安全审核和测试。安全团队还提供安全培训，并积极监控新增安全问题和威胁的报告。要进一步了解如何向海康威视报告问题以及如何订阅安全通知，请参阅

https://www.hikvision.com/cn/support/CybersecurityCenter/。

见远 行更远

See Far, Go Further

微信扫一扫
关注海康威视网络安全

海康威视

www.hikvision.com

客服热线：400-800-5998

股票代码：002415

微博：@海康威视hikvision