

杭州安恒信息技术股份有限公司 2020年度社会责任报告

关于本报告

本报告是杭州安恒信息技术股份有限公司发布的社会责任报告暨环境、社会及管治报告，本着客观全面、规范透明的原则，详细阐述2020年度公司环境、社会及管治工作的管理理念、亮点实践及年度成效。

报告范围：

除特殊说明外，本报告涵盖杭州安恒信息技术股份有限公司总部、分支机构及附属公司，与《杭州安恒信息技术股份有限公司2020年年度报告》对外披露范围保持一致。

时间范围为 2020 年 1 月 1 日至 2020 年 12 月 31 日，部分内容超出此范围。

称谓说明：

为便于表达，本报告中提及的“安恒信息”“安恒”“公司”“我们”等均指代“杭州安恒信息技术股份有限公司”。

数据说明：

本报告关键财务绩效摘自《杭州安恒信息技术股份有限公司2020年年度报告》，其他数据来自公司内部管理体系。

可靠性保证：

公司董事会承诺对报告内容进行监督，确保不存在虚假记载、误导性陈述或重大遗漏。

目录

关于本报告.....	2
报告范围:	2
称谓说明:	2
数据说明:	2
可靠性保证:	2
一、董事长致辞.....	5
安全是温暖人心的力量.....	5
2021 年 4 月.....	7
二、关于我们.....	8
1、治理架构.....	8
(1) 董事与董事会.....	9
(2) 监事与监事会.....	9
(3) 高管.....	9
2、党建工作.....	10
(1) 组织架构.....	10
(2) “红色+”党建品牌介绍.....	11
(3) 特色做法及成果.....	12
3、内控管理.....	14
4、反舞弊.....	15
(1) 制度建设.....	15
(2) 舞弊查处.....	15
(3) 廉洁宣贯.....	15
(4) 风险防控.....	15
三、安恒之道.....	16
1、企业文化.....	16
2、责任体系.....	16
(1) 养兵计划: 齐心协力, 抗震救灾.....	16
(2) 神盾计划: 网络反诈, 刻不容缓.....	17
(3) 星火计划: 十年树木, 百年树人.....	17
(4) 新星计划: 英才汇集, 共襄盛事.....	18
3、利益相关方沟通.....	18
四、从不跟随, 做极致责任的创新者.....	20
1、健全创新管理体系.....	20
(1) 技术微创新.....	20
(2) 功能微创新.....	20
(3) 服务微创新.....	20
(4) 营销微创新.....	20
2、建设创新人才平台.....	21
3、成就科技创新成果.....	21
五、永远赋能, 做持续价值的创造者.....	24
1、股东和债权人权益保护情况.....	24
2、供应商、客户和消费者权益保护情况.....	24

3、产品安全保障情况.....	25
4、公共关系、社会公益事业情况.....	25
六、持续精进，做网安英才的汇聚者.....	26
1、员工权益保障.....	26
(1)创造舒适的工作环境.....	26
(2)未雨绸缪，制定应急预案.....	26
(3)丰富员工福利，确保员工权益.....	26
2、员工培训发展.....	27
3、员工生活关怀.....	31
七、安全基石，做数字经济的助推者.....	34
核心技术进展.....	34
1、云.....	35
(1)基于云架构的安全扫描与监测技术.....	35
(2) SaaS 化云安全防护技术.....	36
(3)云平台融合对接和统一编排管理技术.....	36
2、大.....	38
(1)多协议解析与数据治理技术.....	38
(2)运维访问控制审计技术.....	38
(3) Web 应用透明代理与深度攻击检测防护技术.....	39
(4)基于网络流量的未知威胁及 APT 攻击检测技术.....	40
(5)分布式漏洞发现与验证技术.....	41
(6)大数据深度安全检测与分析技术.....	41
(7)态势感知分析与挖掘技术.....	42
3、物.....	43
(1)全网资产测绘技术.....	43
(2)物联网可信互联与智能防护技术.....	43
4、工.....	44
面向工业控制系统安全的定量评估和全生命周期防护技术.....	44
八、行稳致远，做美好未来的缔造者.....	45
1、守护祖国网络疆土.....	45
2、精准扶贫.....	45
3、人才培养.....	46
4、关爱青少年.....	47
5、抗击疫情.....	47

一、董事长致辞

安全是温暖人心的力量



我常常要和人解释，什么是网络安全。我一直在尝试，让更多的人感受到网络安全的力量。

在过去的 2020 年里，新冠疫情将无措、徘徊暴露，也将转机带到我们身边。去年疫情期间，安恒信息及时制定应急措施，对疫情重灾区求职者开辟绿色通道，为全国合作伙伴提供帮扶措施，安恒密盾护航钉钉，保证

1000 万中小企业在家办公信息安全无忧；安恒信息开展公益保险计划，保障企业不受“信息疫情”……

安恒作为“逆行者”，始终牢记自己的使命，展开的一系列公益行动，全力支持战疫，这都让我们对企业作为企业公民的社会责任有了更深的感悟与理解。道阻且长，行则将至，安恒公益基金会也将持续进行“养兵计划”，保证在第一时间紧急援助灾区、疫区，在面对需要伸出援手的事物和人群面前，安恒人将会毫不犹豫的伸出双手，贡献出自己的力量。

对于安恒而言，责任的承担并非只是高光时刻，而是犹如一条金线贯穿在企业发展的历史长河之中，早已深深根植在组织文化的基因里，同防风固沙一般，在所不辞。

“安于责任、恒于创新”，不断汲取营养。这些年来，凭借优秀的技术研发团队及强大的技术创新能力，我们在应用安全和数据安全等领域实现了多项技术突破，确保了公司在多个相关细分市场处于行业领先地位。相信未来在“新场景”、“新服务”的驱动下，安恒信息将衍生出更多有竞争力的产品和服务，为我国网络信息安全产业的发展贡献更大力量。

作为护佑一方生态屏障的榜样，安恒信息锐意进取。自 2008 年至今，共参与近百场国家重大活动的网络安全保障，圆满完成为北京奥运会、上海世博会、历届世界互联网大会、G20 杭州峰会、厦门金砖峰会、博鳌亚洲论坛、上合组织青岛峰会、武汉军运会等众多重大活动提供网络信息安全保障，并多次承担安保组长、安保中坚力量的职责，确保网络安保工作万无一失。

对于新时代的企业而言，不仅需要以自身良好的业绩来证明其本身的发展能力和潜力，同时也需要以良好的社会责任感来反哺社会，我们深谙此道，并时刻践行。

安恒不忘土壤深处的滋养，积极响应国家关于脱贫攻坚工作的号召，以实际行动践行社会责任，积极投入到扶贫等公益事业中。深度参与“万企帮万村”精准扶贫行动，按照扶贫工作的有关文件精神和工作部署，针对西陇村古茶这一特点，安恒信息与普安县南湖街道西

陇村共建茶产业合作社，在资金、技术、人才、产业发展等方面给予支持和帮扶，帮助西陇村打造“普安红”茶品牌与订单化帮扶政策，达到增收、脱贫甚至致富的愿景。

公司不断探索，2021 年全力打造“安恒港湾”公益基金会官网这一平台，全面开启“养兵”、“神盾”、“星火”、“新星”四大计划。比如，“新星计划”将联合全国各大院校、科研组织组成的专家组，在国内外知名等院校、科研院所范围内，按照技术的突破性、创新性、市场价值等方面评选在基础研究和科技成果产业化领域杰出华人青年科学家，授予“青年科学家新星”称号，并给予资金奖励，为基础研究和科技成果转化提供更全面的社会支持。未来，安恒信息也将继续发挥产业和资本优势，为“新星计划”科学家实验研究、科研项目产业化上提供培育和孵化支持。

除了安全我们想守护更多，像是关爱青少年成长发展，种下安全之果，得成荫风景。安恒信息建有省内第一个网络安全的科普教育基地。目前，已和 20 余家高校合作建立网络安全实验基地，在校园中开展网络安全普及教育活动，通过教学与实验相结合的方式，提高在校大学生的网络安全知识和防护能力，获得了在校师生极大的好评。

过去一年的实践里，安恒坚定战略方向，以人为本，共创社会和谐，努力创造我们共同的美好家园。

安恒信息董事长 范渊

2021年4月

二、关于我们

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于 2007 年，于 2019 年 11 月 5 日正式登陆上交所科创板股票上市，股票代码：688023。自成立以来一直专注于网络信息安全领域，公司秉承“助力安全中国、助推数字经济”的企业使命，以数字经济的安全基石为企业定位，将“诚信正直、成就客户，责任至上，开放创新，以人为本，共同成长”作为企业的价值观，致力于成为一家具有优秀企业文化和社会责任感的新时代网络信息安全产品和服务提供商。

安恒信息以云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大方向为市场战略。凭借强大的研发实力和持续的产品创新，已形成覆盖网络信息安全生命全周期的产品体系，包括网络信息安全基础产品、网络信息安全平台以及网络信息安全服务，各产品线及业务线在行业中均形成了强大的竞争力。

1、治理架构

公司按照《公司法》、《证券法》、《上市公司治理准则》等规范要求，建立了公司治理的各项基础制度框架并有效执行，公司治理较规范，股东大会、董事会、监事会运作规范有效，董事、监事和高级管理人员勤勉尽职，按照法律法规和公司章程的规定履行职权。报告期内，公司召开 3 次股东大会、9 次董事会和 8 次监事会，对利润分配、

对外投资等事项，积极听取独立董事意见；股东大会采取现场投票与网络投票相结合的表决方式，并对与中小股东利益相关的事项采用单独计票；三会的召开、审议均严格履行相关程序，没有出现违规担保、关联方非经营性资金占用等情况；公司及公司相关人员没有因违规运作遭受监管部门处罚的情况。

(1) 董事与董事会

董事长：范渊

董事：陈英杰、姜有为、张小孟、吴卓群、袁明坤、陈英杰

独立董事：赵新建、辛金国、朱伟军

(2) 监事与监事会

监事会主席：冯旭杭

监事：王欣

职工监事：郑赳

(3) 高管

总经理：吴卓群

副总经理：张小孟、袁明坤、黄进、戴永远（兼财务总监）、楼晶（兼董事会秘书）

2、党建工作

(1) 组织架构

杭州安恒信息技术股份有限公司于 2018 年成立党委，下设 7 个党支部，现有党员 130 名。在安恒杭州总部，管理层党员比例占 70%左右，党委班子成员均为总裁办成员。



(2) “红色+”党建品牌介绍

“红色卫士”：安恒党建工作的形象统称，以企业的健康稳定发展为中心，体现行业特点，红色是党旗主色调，象征着党的领导；安恒作为互联网大会的“安全卫士”，肩负起“助力中国安全”的责任与使命，对安保产品精益求精，同时切实加强党员队伍建设，深入贯彻落实“全面从严治党”，努力将党员团结起来，铸造一支政治过硬、业务过硬、责任过硬、纪律过硬、作风过硬的网络安全卫士队伍，净化网络空间，维护网络安全。把党组织建设落实到日常工作的方方面面，在“助力安全中国、助推数字经济”过程中践行党员的先锋模范作用。

“红色卫士”理念贯彻于安恒党委日常的方方面面，一直以来，党委自觉担负起政治责任，坚决维护以习近平同志为核心的党中央权威和集中统一领导，在重大活动任务中冲在一线，以护卫网络安全为己任。安恒党委自成立以来，在各级政府指导下，在北京奥运会、国庆60周年庆典、上海世博会、广州亚运会、抗战七十周年、连续四届世界互联网大会和G20峰会等重大活动重大安保任务中，由党员组建的突击队，起到了先锋带头作用。为深入学习贯彻习近平总书记网络强国的重要思想，深入实施党建高质量发展行动计划，充分发挥党建引领作用，加强网络安全知识技能宣传普及，党员充分发挥榜样带头作用，发扬吃苦耐劳的优良品德，认真负责完成每一次安保任务，共筑网络安全防线。

（3）特色做法及成果

红色卫士的特色亮点。每年的特殊节日，如七一建党节，公司都会组织党员及全体员工参与志愿献血活动。献血活动中，每个献血者都将浓浓爱心化作汨汨热血，以实际行动助力无偿献血事业，充分展现了安恒人关爱他人的精神面貌，彰显了党员干部服务社会的时代精神。



扶贫项目是安恒党员活动的重点。安恒党委采取多地开展，因地制宜的方式带领党员们深入贫困村实地查看了扶贫项目实施情况，了解近期的生产生活情况，积极宣传党的方针政策，并给出对应解决方案，共同想办法促增收，努力改善生产生活条件，争取早日脱贫。

安恒大学致力于构建产、学、研对接桥梁，为国家及各行业提供力所能及的安全服务与人才培养。公司内部成立安恒大学，协助公司创新人才进行职业生涯规划，建立包括人才等级评聘、岗位任职制度、重点员工培养计划等，使公司创新人才在发展方向上，拓宽发展面，保证核心骨干员工的稳定。其中涉及线上教学+线下开课。

雏鹰训练营是安恒人才培养的重要组成，经过历年的实践与完善，已形成独具安恒特色的新员工培养模式，包括野外大作战、室内大比拼等新兴模式。为帮助应届学员扫除新入职场的困惑与迷茫、快速转变

角色、融入职场大环境，并增强新员工归属感，安恒人力资源部、党委协同各下属业务板块共同开展雏鹰训练营。该训练结合武装培训，在训练过程中，党员们起到了“领头鹰”作用。

安恒党委以“服务型”“学习型”“示范型”“创新型”“实干型”“链接型”六大抓手，建设特色党组织，鼓励党员下乡扶贫活动、构建安恒大学、开展雏鹰计划等活动。





3、内控管理

为推动内部管理体系的有效落地，安恒信息根据各业务模块的流程风险梳理形成《企业内部控制流程手册》，并通过开展日常审计对内部

控制建立和实施情况进行监督检查。

4、反舞弊

安恒信息向来重视反舞弊工作，主要从制度建设、舞弊查处、廉洁宣贯、风险防控等方面着手，努力营造“阳光透明、诚信共赢”的合作环境和“风清气正，阳光同行”的职场环境。2020 年，安恒信息反舞弊工作成果良好：

（1）制度建设

先后制定并持续完善《安恒廉洁诚信制度》、《安恒举报奖励制度》、《安恒员工亲属回避制度》等制度，确保公司内部反舞弊工作和员工日常行为有规可依。

（2）舞弊查处

通过舞弊案件查处，向舞弊人员“亮剑”，向舞弊行为说“不”。

（3）廉洁宣贯

通过廉洁文化宣贯，引导内部员工强化廉洁意识、践行诚信正直价值观。2020 年，廉洁活动周、国际反腐日、新员工廉洁培训、自制短视频、自制微电影等。

（4）风险防控

以案促防，通过舞弊案件反推和日常核查发现，梳理流程和管理漏洞，采取相应措施，规避舞弊风险和其他重大风险。

三、安恒之道

1、企业文化

使命：

助力安全中国 助推数字经济

愿景：

成为一家具有优秀企业文化和责任感的新 时代网络信息安全产品和服务提供商。

核心价值观：

诚信正直、成就客户、责任至上、开放创新、以人为本、共同成长

2、责任体系

在过去的一年内，安恒信息成立两只公益基金，分别是“成都市安恒公益慈善基金会”、“杭州安恒公益基金会”（统称为“安恒公益基金会”），依托“安恒港湾”公益基金会官网这一平台，全面开启“养兵”、“神盾”、“星火”、“新星”四大计划。

（1）养兵计划：齐心协力，抗震救灾

在 2020 年初，面对让人措手不及的新冠肺炎疫情，安恒信息始终牢记自己的使命，及时制定应急措施，对疫情重灾区求职者开辟绿色通道，为全国合作伙伴提供帮扶措施，安恒密盾护航钉钉，保证 1000

万中小企业在家办公信息安全无忧；安恒信息开展公益保险计划，保障企业不受“信息疫情”。

道阻且长，行则将至，安恒公益基金会将持续进行“养兵计划”，保证在第一时间紧急援助灾区、疫区，在面对需要伸出援手的事物和人群面前，安恒人将会毫不犹豫的伸出双手，贡献出自己的力量。

(2) 神盾计划：网络反诈，刻不容缓

安恒信息已成立全国首个网络反诈骗实验室，协助公安部门侦破包括部督在内的大案、要案数百起，累计涉案人员数千万、涉案金额超千亿。安恒公益基金会将此次为基础，启动“神盾计划”，开展线上科普，全力打造《一个懂安全的朋友》系列科普视频及线下反诈骗公益活动，同时有针对性的对遭受网络诈骗的家庭给予帮扶。

(3) 星火计划：十年树木，百年树人

安恒公益基金会将通过“寻梦亚运网络安全卫士”、“大运会网络安全志愿者联盟计划”来提升学生攻防兼备的网络创新实践能力，培养学生的创新意识与团队合作精神，增强学生信息安全意识，提高学生的网络空间安全创新能力与实践技能。

与此同时，安恒公益基金会与公安部三所、中国信息安全测评中心、中国网络安全审查技术与认证中心等部委、机构合作，共同提升我国网络安全治理水平和网络安全人才综合技能水平，为国家发展和社会经济建设培养各层次网络安全人才。

(4) 新星计划：英才汇集，共襄盛事

“新星计划”将联合全国各大院校、科研组织组成的专家组，在国内外知名等院校、科研院所范围内，按照技术的突破性、创新性、市场价值等方面评选在基础研究和科技成果产业化领域杰出华人青年科学家，授予“青年科学家新星”称号，并给予资金奖励，为基础研究和科技成果转化提供更全面的社会支持。

未来，安恒信息也将继续发挥产业和资本优势，为“新星计划”科学家实验研究、科研项目产业化上提供培育和孵化支持。

3、利益相关方沟通

利益相关方	利益相关方期望	安恒信息回应方式
客户	合同履行 产品质量安全 提供优质服务 保障客户隐私	首席客户成功官 客户拜访 客户满意度调查 电话、邮件、信件及 在线反馈
员工	基本权益保障 民主管理 良好的办公环境 良好的工作氛围	遵守相关法律法规 安恒社区、吐槽大会、总裁直通车等沟通平台 新建办公大楼 推进企业文化在公司内部的传播和融入
股东	了解公司经营现状 基本权益保护	股东大会 定期报告和公司公告 加强风险监控、防范和应对

<p>市场</p>	<p>能力提升 公平竞争 引领网络安全发展 更多专业的网络安全人才</p>	<p>主办或参与行业研讨会 推动诚信网规体系建设 西湖论剑网络安全大会 网络安全空间学院</p>
<p>政府</p>	<p>守法合规 推动经济发展和转型 促进社会就业</p>	<p>严格遵守各项法律规范 与政府部门合作探讨创新模式 合作特色中国项目 积极响应政府各项政策</p>
<p>社会</p>	<p>促进就业 促进社区发展 扶贫救灾</p>	<p>提供创业平台 支持公益组织发展 提供公益平台 参与公益活动</p>
<p>环境</p>	<p>遵守环境法律法规 践行节能减排 资源节约利用 环保意识提升</p>	<p>环保技术应用 环保理念宣贯 环境信息公开</p>

四、从不跟随，做极致责任的创新者

1、健全创新管理体系

鼓励多种的创新模式

(1) 技术微创新

满足用户的某种需要，或给用户带来独特体验出发进行周期短、应用快的技术创新、改良或运用，就是技术型微创新的核心，快速提升产品竞争力

(2) 功能微创新

创造具有全新功能的产品的或服务，在原有产品的基础上增加了全新的附加功能。

(3) 服务微创新

改进并且设计提供满足用户体验的决定性要素。通过端对端周到而有特色的服务，营造出良好的用户体验

(4) 营销微创新

在营销环节，采用新的手段，新的形式。达到促进销售的作用，对产品也服务根据客户需求进行创打包服务

2、建设创新人才平台

安恒信息已与国内近百家高校开展了专业共建、实验室建设、师资培训等校企合作项目，其中在大数据、云安全、物联网、工业互联网等多个专业都有深入的科研合作与协同育人，致力于以产教融合带动科技创新和技术成果转化，推动校企产学研深度合作。

同时，联合中国信息安全评测中心共同运营 CISP-ICSSE（注册信息安全专业人员-工业控制系统安全工程师）等培训，向社会输送了超万名信息安全专业人员。

每年举办西湖论剑中国杭州网络安全技能大赛，发掘人才、汇聚人才，打造平台、内容、服务三位一体的完整人才培养体系，为网络安全人才培养提供充分土壤，赋能全国数字经济安全基石。

3、成就科技创新成果

2020 年 4 月，发布明鉴迷网系统新版本，系统提供丰富的高低交互蜜罐类型，包括 web 服务蜜罐、操作系统蜜罐、数据库蜜罐、系统服务蜜罐、中间件蜜罐、工控蜜罐、物联网蜜罐等，可泛化上千种蜜罐节点，提升网络复杂度。另外，可以通过在真实业务系统上安装流量转发 Agent，将攻击流量重定向引流至蜜罐网络中，来扩大诱捕覆盖面。为保证系统具有更逼真的“用户体验”，系统利用模拟网络流量、仿真业务系统界面、虚拟数据、高度伪装内容等手段，让诱捕陷阱看起来更加“可口”，进而提升对攻击者的吸引力，获取攻击者的注意，延缓攻击进程，达到诱导、捕获攻击者的目的。

2020 年 5 月“安恒 EDR 新版本”发布，根据 ATT&CK 理论，对攻防对抗的各个阶段进行防护，包括单机扩展、隧道搭建、内网探测、远控持久化、痕迹清除。高级威胁功能不仅可以做到威胁攻击审计，还可以防止黑客渗透攻击，实现攻防对抗 360 度防御。

随着信息化的发展，物联网广泛应用于生活、教育、政府、消防、医疗、酒店等各个领域。物联网的终端数量多、类型复杂，导致了其面临多样化的安全威胁，包括木马、间谍软件、劫持攻击、拒绝服务、数据泄露、文件上传等。一旦这些业务和应用被攻击，相关信息和数据被窃取或伪造，都可能对国家安全、社会秩序、公众利益造成不同程度的侵害。

2020 年 7 月，基于“平台+端”联动的物联网安全态势感知与管控平台，物联网安全态势感知与管控中心 V2.1 发布。物联网安全态势感知与管控中心面向物联网终端安全监控、数据加密与态势感知，采用“平台+端”结合的联动式动态预警技术、内核级进程文件防护技术、智能自学习威胁感知技术等多项关键技术，对物联网终端进行数据加密、威胁感知和安全加固，结合各子引擎安全信息上报、数据大脑威胁情报，实时感知海量物联网设备的安全状态、威胁及非法接入等整体情况。

2020 年 8 月，公司全新推出网络资产综合治理平台。该平台集资产探测、风险监测功能于一体，能够有效帮助用户摸清单位网络资产底数，建立网络资产档案库，从域名、主机、web 应用等多维度实现网络资产状态及风险的可查、可知、可控，为日常网络安全管理工作提

供便利。平台可适用于高校、公安、大数据局、电子政务办、运营商网运部、集团企业等多个客户与场景。

2020 年 9 月，公司发布集多云管理和多云安全管理于一体的一站式服务平台-安恒云。伴随着云计算技术走向成熟以及用户对成本、备份等多类诉求，“多云”的趋势已经非常明显，但又不可避免地面临资源分散、难以管理等问题。安恒云能够把用户的多云环境串联并统一运维、统一管理，助力用户公平选云、安全上云、便捷管云、实惠用云，为用户数字化转型提供多云管理能力和安全能力。

五、永远赋能，做持续价值的创造者

1、股东和债权人权益保护情况

公司重视维护股东权益，积极回报投资者。2019 年 11 月 5 日，公司完成首次公开发行股票并在上海证券交易所科创板上市。为股东和投资者创造更大的价值，是公司不断发展和成长的巨大动力。公司严格按照《公司章程》和《公司未来三年（2019-2021）股东分红回报规划》制定了公司2020年度利润分配方案，给予投资者合理的回报；通过接待现场调研、公开电话和邮箱互动、面对面交流等多种途径与投资者进行沟通，增强投资者对公司的了解。2020年度信息披露及时、真实、准确、完整，无应披露而未披露事项。

2、供应商、客户和消费者权益保护情况

公司坚持“诚信正直，成就客户”的经营理念，积极建立与供应商、客户、消费者之间的长期良好的合作关系。对于供应商，公司注重双方的沟通和协调，严格遵守并履行合同约定，恪守商业信用；对于渠道经销商客户，公司持续拓展和巩固双方战略合作关系，为他们提供有竞争力的产品和完善的配套服务和培训体系，共同发展，实现互利共赢。对于直销客户，公司注重倾听对方的诉求和反馈意见，及时协调并处理，同时总结工作和产品上的经验和教训，持续提升客户满意度和公司品牌竞争力。

3、产品安全保障情况

公司自成立以来，始终重视产品质量和售前售后服务保障，希望赋予客户最好的使用和服务体验。目前公司在总部、全国各省、市、自治区和直辖市有专业完善的服务支撑体系，可提供便捷、高效、快速、专业的响应支撑服务。依托自身在网络安全大数据方面强大的服务能力，公司为各地公安、网信、通管、经信等监管机构提供技术支持和保障，同时开通了7×24小时安全运营、线上线下安全教育、安全预警与通告、7×24小时实时在线安全监测防护等服务。

4、公共关系、社会公益事业情况

公司始终牢记“助力安全中国，助推数字经济”的企业使命，致力于我国网络信息安全产业的发展，牵头或参与多个重大项目活动。报告期内，公司通过注重网络安全生态圈的构建，与政府、机构、高校、企业等建立了良好的战略合作关系，并为全国、省级、市级近百场网络安全赛事提供技术支撑，累计参赛者超过2万人次。此外，公司联合中国网络安全审查技术与认证中心、中国信息安全测评中心、教育部教育管理信息中心等多个部委，组织开展了近百场的网络信息安全培训。

六、持续精进，做网安英才的汇聚者

1、员工权益保障

公司追求企业与员工共同发展，尊重人、关心人的企业文化成为安恒信息事业的重要推动力。

(1)创造舒适的工作环境

公司全面导入质量、环境、职业健康安全管理体系，严格遵守国家《劳动法》、《安全生产法》等相关法律法规，逐层签订安全管理目标责任状，定期开展消防演练活动，通过改善作业条件逐步加强劳动保护。

(2)未雨绸缪，制定应急预案

为确保生产经营工作的稳定性、连续性，针对生产工作中常遇见的突发事件，公司配备各种应急设备，如照明设备、消防设备、通讯设备。当可能发生危险情况或紧急状况时（如台风、洪水、火灾），迅速启动相应应急预案，安全生产管理委员会随即发挥组织、指导作用，深入现场，了解实情，制定相关的保障措施做好物资准备工作，以人为本，保障员工的利益，尽可能减少生产损失，保障生产有序开展，尽量满足顾客对产品的消费需要。

(3)丰富员工福利，确保员工权益

公司福利

法定福利

基本养老保险、基本医疗保险、失业保险、工伤保险、生育保险
保障福利

工作餐补、节假日福利、健康体检、高温补贴、通讯补贴等

激励福利

职称奖励、年度绩效奖励、内外培训机会

其他福利

结婚喜金、生育喜金、季度劳保、节日礼品（圣诞节、中秋、三八节）、
职工子女升学安排等

2、员工培训发展

根据公司战略发展需要，不断提升员工素质和能力，打造符合业务发展需要的组织能力。

根据不同职位族和不同层级人才的特点，以人才梯队建设为手段，实施多元化培养方式。通过人才培养培养，使人才的知识结构、技能方法、工作价值观日益提高，在不断提升个人价值的同时，推动组织向前发展，最终实现组织与个人的双赢。

1、员工的教育与培训

1) 培训需求调查及计划制定

基于公司年度经营目标，参照岗位胜任能力模型，在平衡长短期目标与员工发展、个性化需求与职业生涯发展需求的基础上，公司人力资源部每年12月至次年1月期间进行分层级、分类别的培训需求调查，

通过问卷、访谈等形式收集培训需求。

2) 培训实施

① 内部培训

各部门负责各类培训项目的组织实施，人力资源部做好相应支持，并做好培训工作记录。同时，公司成立网络空间安全学院，依托公司自身领先的产品和服务，把产业资源、行业案例，以及成熟的项目经验进行整理，并相应转化为教育资源，实现公司内部知识沉淀和传递，使技术人员能够通过在线学习和练习，掌握最新的安全检测与防御能力。通过公司业务对接安全服务实际需求，使安全技术人员在承担安全服务，理论结合实践进行检验；构建在线考核和竞赛服务平台，通过多轮考核竞赛的方式使技术人员对自身水平有精准定位，为安全服务人员进行技术能力画像；与各类招聘网站进行在线对接，为安全人员进行第三方能力背书，在为公司培养安全专业技术人才的同时，也能够实现对外培养输送。

② 外部培训

公司在自身培养网络信息安全类专业技术人才的同时，还与全国60多所高校建立了各种形式的校企合作，协助培训专业网络信息安全人才，包括像浙江大学、北京航空航天大学、哈尔滨工业大学等985高校一起培养高端网络信息安全人才，也与温州职业技术学院、杭州职业技术学院等专科类学校培养网络信息安全一线工程师队伍，为完善国内网络信息安全人才梯队做出贡献。

3) 培训效果评估

公司重视培训的效果评估、转化、应用、传播与固化，以调查问卷的方式对课程、组织方式及培训效果进行评估，将培训满意度等指标纳入培训效果考核，并通过情景模拟、实战检验等形式进行培训效果二次评估，加强培训工作的有效性。

4) 培训改进

公司重视培训体系优化和改进工作，在培训方法和资源管理上不断进行改进提升。第一，加强内训师团队建设，通过赋能内训师技能，不断优化内部培训效果；第二，加强课程管理，通过组织课程开发与评审，不断提高内部培训课件内容质量。第三，加强案例输出，通过实战化案例研讨和编制，不断提高教学内容的有效性。第四，加强考试管理，通过理论、实操考试测验方法的改良改进，不断提高教学质量的检验能力。

2、员工职业发展

从称职胜任角度出发，针对特定的工作领域，对员工能力和贡献分等分级，通过方法和工具建立起任职资格标准，以任职资格标准规范员工的培养和选拔，建立员工职业发展通道，牵引员工不断学习，同时为员工晋升管理、薪酬管理等人力资源工作提供重要依据。

根据职业发展双通道模型，所有岗位划分为专业序列和管理序列，按照相似职能分类，分为销售族、产品族、研发族、技术族、研究族、服务族、供应链族、项目族、职能族、管理族10大职位族，并根据职位族、职类、子类对所有职位进行划分和归类。

依据所要求的知识、技能的不同；所解决问题的难度、复杂度、熟练

程度和领域的不同；在本专业领域内的影响力不同；对流程优化和体系变革所起的作用不同；所承担的责任大小不同，将职业发展通道划分为以下层级：

P&M双通道职业发展体系

公司每年会组织全员任职资格晋升工作，对符合条件的员工通过答辩、沟通等形式进行评审，为员工的职业发展和晋升提供多维度的建议，帮助员工建立清晰的职业发展规划。

员工职业发展路径包含纵向发展、横向发展的职业发展道路，体现了多通道发展特征。

1、纵向职业发展通道：包含管理类职务晋升和专业技术类职务晋升两种形式。P序列内除专家级和研究员级外，普通等可以晋升为同层级的职业等，职业等可以晋升为上一层级的任何一个职等；P序列内专家级和研究员级，职业等可以晋升为同层级的职业等+，职业等+可以晋升为上一层级的任何一个职等；

2、横向职业发展通道：分为专业序列内跨职位族转岗，以及专业序列转向管理序列；

3、岗位调整：绩效符合公司要求并积极上进的员工有机会得到不同职责范围内的工作岗位。岗位调整包括轮岗、换岗，岗位的调整须符合新岗位任职资格要求；

4、管理与专业之间转化：非技术研发性部门：员工不仅可以选择在各自的专业方向或管理方向上发展，还可以在专业和管理之间转换。

从专业转为管理：承担管理序列的职位首先需有专业的认证，满足M

级别对应的最低专业资格等级；其次考察是否符合管理岗位的胜任要求。从管理转为专业：建议为管理级别所对应的专业层级。以上出现特殊情况的，由人力资源部发起任职资格评估流程。

a) 人才梯队建设

公司重视各层级优秀潜力人才的挖掘与培养，打造金字塔型的人才梯队建设，建立组织人才盘点机制，盘点、评估结果将作为公司选贤用人的重要基础。

公司建立了一套适合自身发展的“造血机制”。在管理序列上，从应届生新员工、社招新员工转身培训，到中基层管理者培训，再到高层管理者培训，形成人才梯队赋能。在专业序列上，公司重视员工的技能提升，实施技术线培训、导师制度、半月谈会议、项目开发研讨、提报会、完善技术人才激励制度、项目奖制度、创意提案等。并通过引进技术型人才，开展内部培训，提升整体的技术人员水平。

b) 职业发展标杆

公司逐步建立职业发展成功典范，并设立人才标杆，让全体员工学习，坚持做好以老带新，青出于蓝而胜于蓝，挖掘团队中的两种力量——榜样的力量、标杆的力量，以提高员工的积极性，与进取心。

3、员工生活关怀

1、公平合理的薪酬体系

公司根据战略发展规划，及结合市场薪资水平和各岗位的价值等因素，建立了一套导向奋斗的全面薪酬体系。公司薪酬体系遵循“以

奋斗者为本”的理念，从物质激励、精神激励、平台激励三个方面进行体系性设计，为员工提供360度激励和关怀。

图 公司全面薪酬激励体系

1) 物质激励:

公司根据不同岗位工种特性设立不同的工资结构，包括基本工资、绩效奖金、项目提成、特殊奖励和年终奖，在保持行业竞争力的同时，有效发挥激励牵引作用。同时，在依法依规提供法定福利的同时，公司提供不同维度的人性化补充公司福利，以及各类专项补贴，为员工薪酬收入提供多维度的保障和支持。

2) 精神激励:

公司在物质激励建设之外，非常重视精神激励建设，充分体现“马斯洛需求层次理论”在员工激励上的应用。通过各类先进员工表彰、各类员工关怀机制，突出公司“以奋斗者为本”理念的切实行动。

3) 平台激励:

公司通过不断加强机制和平台建设，提供良好的软硬件工作学习环境和氛围，提供各类学习机会，帮助员工做好职业生涯规划 and 晋升，以不同角色参与到公司管理经营建设，为员工提供“参与共享、成长收获”的职业发展平台，促进员工更好地奋斗和贡献自身价值。

2、员工满意提升

公司关注员工满意度的提升，不断完善员工活动场所及设施、丰富活动内涵，提升员工满意度，促进活力团队的塑造。安恒计划设计员工满意度调查表，进行全员的满意度调查，并利用调查表提升改进公司

的环境与管理，让大家真正的“干在安恒，爱在安恒，学在安恒，成在安恒，乐在安恒”。

七、安全基石，做数字经济的助推者

报告期内新技术、新产业、新业态、新模式的发展情况和未来发展趋势。

由于近年我国云计算、大数据、物联网等新技术的快速发展，在推动新兴技术市场不断增长的同时，也催生了新的安全需求和新的应用场景。

新技术、新场景下，防护对象改变，企业网络边界逐渐消失，政府和企业网络信息安全防护理念发生较大变化，网络信息安全不再是被动修补模式，而是与信息系统建设同时规划。随着新的应用场景包括云计算、大数据、物联网和移动终端等的普及，企业信息化程度逐步提升，网络信息安全领域出现了三大变化：从传统 PC、服务器、网络边缘到云计算、大数据、泛终端、新边界；防护思想从“风险发现、查缺补漏”转变到“关口前移、系统规划”；核心技术升级从传统的围墙式防护到利用大数据等技术对安全威胁进行检测与响应。

核心技术进展

核心技术及其先进性以及报告期内的变化情况

凭借优秀的技术研发团队及强大的技术创新能力，公司在应用安全和数据安全等领域实现了多项技术突破，截至报告期末，公司共拥有48项核心技术，其中22项是公司基于云安全、大数据安全、物联网安全和智慧城市安全等新兴安全领域进行深入研究积累所得，该等核心技术确保了公司在多个相关细分市场处于行业领先地位。公司现有核心

技术按照技术应用方向主要可以分为13项大类技术，报告期内，公司主要针对现有核心技术进行优化，该等核心技术先进性及产业应用情况具体如下：

1、云

(1) 基于云架构的安全扫描与监测技术

业界的安全检测技术主要通过硬件盒子方式实现，检测能力受硬件性能限制，存在慢报及误报等问题。公司基于云架构的安全扫描与监测技术是国内首批运用SaaS模式进行安全检测的技术。该技术基于网站安全领域的安全事件监测技术，通过运用机器学习技术对全国670万 ICP 网站首页抽检样本进行分析、训练，能够实现文本语义准确分析识别，并结合公司威胁情报能力有效解决了孤链监测问题，丰富和扩展了黑名单库，大幅降低监测误报率并提升检测范围，能实现大容量、高并发、高准确率、高检出率的网站实时监测。该技术能做到检测数据完全自动标签化，自动化数据校验率达到 90%以上，当前监测网站数量峰值达到 1,096,725 个(次)/天，平均监测值约为 476,880个(次)/天。相比较传统安全事件监测技术，公司的监测技术依托云端大数据能力处理分析海量安全事件样本，监测发现率不低于 95%。目前国内掌握同类技术的企业主要有知道创宇、奇安信等，公司监测技术在发现率和准确率上有较大优势，处于领先水平。

（2）SaaS 化云安全防护技术

业界的安全防护产品主要通过硬件方式，部署运维困难，防御能力受设备性能限制，检测误报率高且较难发现复杂的黑客攻击，难以对超大流量DDoS、新型攻击进行防范。公司基于SaaS化云架构的安全防护技术在用户端无需部署任何软硬件，通过网络接入系统后，即可为用户提供远程实时安全防护，网络层最大清洗能力达到2.5T/s DDoS。该技术区别于传统规则检测，通过自然语言处理和人工智能深度学习算法对云端每日22.8 亿次访问数据进行采样分析，能够大幅提高召回率，降低误报率，2020年度识别扫描 IP 69.4万个，每天拦截扫描攻击近1.3亿次，误报率仅为 1%，实现对入侵、篡改、数据窃取、CC等多种攻击的防护，技术领先性受到学术认可，曾被《信息安全研究》期刊收录，是国内首批运用云端威胁情报能力进行防范的技术。该技术利用云端每日十亿级的访问数据采样分析过程进行模型训练，可以周为单位快速迭代优化自身安全检测算法，而传统安全防护技术并不具备该等庞大的云端数据基础支持。随着时间推进，公司该项技术将进一步拉开与业界主流的传统防护技术的性能差距。

（3）云平台融合对接和统一编排管理技术

目前业界云平台的 API 开放性、标准性较低，导致众多云安全解决方案和云安全产品难以交付、使用复杂、防护效果较差。公司是国内首批开展和云平台对接融合的安全厂商，已与华为云、浪潮云、OpenStack等3家国内主流云服务商完成对接融合，并在此基础上研发

提炼了一套云平台融合对接和统一编排管理技术。该技术可实现云管理平台、云安全管理平台、云安全产品三者的统一认证、授权、监测及管理，能够将安全产品与云平台的对接时间控制在 10 天左右，而行业平均对接时间在 30 天以上，单个安全模块的交付时间从数十分钟缩短到 60 秒以内。

该技术采用软件定义网络和容器化技术，相对同行业安全公司的手动编排和引流技术，实现了资产安全防护和安全流量路径的自动化编排，使得云上安全使用更加灵活简易。目前该技术能够兼容国内主流云平台，支持不同云平台的统一用户和管理，在对接效率、编排能力方面国内领先，云平台的对接成功数量，落地的实际案例也处于领先地位。公司与华为云、浪潮云融合对接的云安全解决方案，通过获得了 CSA 云安全联盟和公安部第三研究所的测评认证，获得了颁发的云计算产品信息安全认证证书和 CSA CSTR 增强级证书和云计算产品信息安全认证证书（增强级），是业界首例安全厂商和云平台厂商融合对接云安全解决方案家的联合认证。

目前该技术和华为云、浪潮云版本基本保持同步更新迭代，平均迭代周期为一个季度。由于目前国内云平台标准化、开放性较低，要建立一套能够适配多云的对接方案，并提炼出标准 API 具有较高的技术难度。同时，云平台的融合具有较强的兼容依赖性，云平台厂商迁移成本高，因此该技术不可替代性较高，先发优势明显。未来该技术将向自动化、数据融合、接口标准化发展。同时，平台内云安全组件向轻量化发展，公司后续将探索云安全组件的全容器化，提升资源利用

率和跨云平台的支持，以满足未来公有云和混合云的云安全防护需求。

2、大

(1) 多协议解析与数据治理技术

目前业界传统的数据解析与治理手段，主要基于静态的协议解析规则进行匹配，难以从云环境获取流量进行解析，无法实现对数据解析精准度的动态优化调整，公司该技术实现了对协议解析内容的动态跟踪，进一步反馈闭环调整提升了数据解析准确率，适用于VMware、阿里云、华为云、天翼云等90%以上国内外主流云环境，在协议解析识别广度（物理环境与云环境）、协议识别深度（协议行为特征、传输内容特征等）、协议检测精准度（数据库操作行为、邮件病毒、邮件域名、邮件附件别名等）较传统技术而言具有较大的优势。当该技术应用于数据库行为审计和邮件行为审计时，能实现对数据库操作行为数据和邮件行为数据的全方位解析，公司基于该项技术的日志审计产品市场占比排名第一、数据库审计产品市场排名第二，达到国内先进水平。

(2) 运维访问控制审计技术

该技术可实现各种传统环境、专有云、公有云平台等各类资产的运维接入，一机多用降低了企业内控建设的成本。基于该技术的深度协议代理解析引擎能够兼容支持市场上3200多种不同品牌及版本的资产

设备，相比业内通用的协议有损还原，该技术可100%还原协议细节特性及运维操作过程，保证了审计日志的权威性，是业内领先的运维审计控制技术，公司基于该项技术的运维审计产品目前市场占比排名亚太区第一。

目前该技术已经趋于成熟，迭代周期为 6-9个月，技术的核心难度在协议代理兼容性、业务模型、用户运维习惯、统一认证平台、资产管理平台集成等方面的实践积累，短期内很难实现与该技术相当的功能水平，替代难度较大。

(3) Web 应用透明代理与深度攻击检测防护技术

该技术主要应用于透明网络环境下的各种 web 攻击检测，在网络接入层面兼容性强，转发性能相比于传统内核态转发技术，具有快速转发、低时延等优势，最高单机可处理 10Gbps 的应用层转发任务。基于该技术的用户态协议代理引擎具备实时双向数据包检测的能力，能识别包括无特征的攻击行为及 0day 攻击行为等在内复杂攻击行为，提升 Web 攻击防护准确率。

该技术大幅提升了公司 Web 应用安全产品的业务兼容性 & 数据包代理转发的性能，降低了攻击检测的误报率和漏报率，有效弥补了传统特征引擎检测技术高误报、高漏报等缺点，帮助公司 WAF 产品获得领先的 Web 攻击检测能力，目前市场占比排名第二。目前该技术日趋成熟，技术架构迭代周期约为 6 个月，攻击行为检测迭代周期 1-7 天。该技术需要在网络数据包快速转发、业务兼容、攻击检测算法模

型方面大量实践经验积累，很难在短期内有较大的技术突破，替代难度较高。

(4) 基于网络流量的未知威胁及 APT 攻击检测技术

基于对样本的动静态分析及基因图谱分析能力，该技术能有效发现 0day 样本及变种木马。在动态沙箱检测恶意文件领域，该技术通过对 Windows 文件过滤驱动实现文件重定向等功能，使沙箱具备防虚拟机检测、防调试器检测和防钩子检测等能力，共 200 种防逃逸机制、近似零时间消耗的快速还原检测环境的技术及单沙箱并发检测多个样本的能力，目前单沙箱一天可检测非 PE 文件达 4000 个，根据不同文件类型，一套沙箱系统一天可检测文件 12 万以上，处于业界领先地位。该技术涉及的 Windows 内核层隔离模块在所有内核驱动开发中属于难度层级高、文档资料少的领域。因 Windows 系统的闭源特点，部分功能开发甚至需要逆向工程技术并配合复杂的调试过程，精通该类内核开发、调试并兼具逆向工程的高端开发人才稀缺，使得该技术具备较高的准入门槛；同时该技术包含的基因图谱分析需要通过对大量恶意样本进行深入分析和归纳，并通过软件块化、片段化、归一化及数据库存储和搜索技术来制定软件基因库，由于相关的二进制分析高度专业性以及收集大量恶意样本所需的渠道与时间成本，使得该技术准入门槛很高，可替代性较低。

（5）分布式漏洞发现与验证技术

相较业内同类技术，该技术具备漏洞发现率高、误报率低、对目标系统运行影响低等特点，凭借公司积累的40,000量级漏洞库实现业内领先的漏洞覆盖率。该技术通过分布式扫描方式加快了漏洞扫描速度与稳定性，扫描速度较传统技术提升30%，同时利用动态流量控制方式减少了扫描对目标系统的影响。公司安全研究院借助该项技术多次在全球首先发现包括JAVA框架Struts2的S-045、S-046等在内的重大漏洞，基于该项技术的漏洞扫描系列产品目前市场占比排名前三。

该技术的迭代频率一般与漏洞挖掘的频率和网络公开漏洞的频率保持一致，通过实时爬取网络漏洞的方式，进行每日自动更新。由于该类技术的漏洞发现率和误报率性能改良需要掌握大量渗透测试技术、网络爬虫技术、流量控制技术以及代码语言特性的分析技术，壁垒较高，可替代性低。

（6）大数据深度安全检测与分析技术

业界传统的安全检测手段主要基于静态的策略规则匹配，一般采用阈值触发、关键词触发、情报对比触发等手段，存在数据量小、检测手段单一、时效性差、分析结果准确度低、风险事件定位难等问题。公司在国内率先提出安全分析模型自适应理念，并在产品中实现功能化。相比业界通用的安全检测分析技术，该技术在国内率先实现周期性异常事件检测，解决了多源异构数据的快速复杂关联分析与检索问题，并利用基于机器学习的扫描 IP 分类、策略自学习和优化、DGA

域名快速判别等 100 多个安全场景识别方法，能够实现多维度、细粒度的安全事件分析与跟踪，大幅提升风险定位的准确度，公司基于此项技术产品已发布多个迭代版本，技术处于国内领先水平。

（7）态势感知分析与挖掘技术

业内大多态势感知技术或产品仅停留在基于日志搜集统计可视化或网站漏洞扫描统计可视化阶段，以少量维度的数据采集手段，加上简单的统计排序分析手段，配以可视化页面，实现初步的态势感知功能。公司大数据态势感知分析与挖掘技术真正围绕网络安全态势感知的三要素：态势获取、态势理解和态势预测，以发掘深度威胁和隐患为目标，对能够引发网络安全态势发生变化的要素进行全面、快速、准确地捕获和基础分析。相比业内同类技术，该技术具备实时在线还原恶意样本和域名能力，通过使用内置威胁情报匹配辅助验证功能，使流量的有效识别率提升至 99%以上，告警准确率达到 90%以上。并为恶意样本提供沉浸式的运行环境和无感调试，大幅降低恶意样本的反调试成功率，从恶意特征匹配转变为基于样本异常行为检测技术，该技术处于国内领先水平。基于该技术的态势感知平台产品在实战中多次输出具有重要价值的网络战情报，尤其是在重大活动网络安全保障期间多次输出黑客攻击的预警和攻击的发现。威胁线索分析和网络攻击追溯能力处于领先水平，对同源黑客的追踪和匹配上准确率达到 95%。

3、物

(1) 全网资产测绘技术

该技术旨在探测全球联网资产信息及脆弱性，提供安全感知、威胁预警以及风险检测能力。该技术结合大数据处理算法能实现高并发、低时延、全网覆盖、快速迭代的网络信息数据收集，并发探测速度达到60万每秒，能够识别分析20万种设备及300多种协议，在2小时内可完成全网探测。相比传统网络扫描技术，公司全网资产测绘技术采用大数据群集架构、插件化开发方式，具备更好的兼容及探测性能。该技术迭代紧跟新协议的应用、新安全漏洞发现频率，与全网资产及前沿技术产品紧密相关，需要对全网资产通讯协议及设备指纹进行长期持续的分析 and 数据积累，以覆盖大量通讯协议及 IP 数据，技术门槛较高。目前国际范围内同类技术主要有 Shodan 和Zoomeye，公司该项技术在识别指纹量、并发的探测速度方面有较大优势，处于国际领先水平。

该技术是目前新兴的全球联网设备探测技术，未来主要向支持所有已知工控协议、物联网协议、网络通信协议的资产探测发展，并不断积累指数级别增长的全网实时数据，从而提升实时威胁预警、全网态势感知、精确脆弱性分布探测能力。

(2) 物联网可信互联与智能防护技术

该技术具备较强的跨平台能力和较好的可移植性，能够实现端到端的

安全加密，密钥分发能力高达 20000 次/S，单次加密延时低于 1.66ms，对终端数据传输效率几乎无影响。相比于传统网络层安全防护技术，该技术可以深入物联网终端内部进行安全防护，通过驱动级安全防护结合云端智能分析的防护能力构建完整的物联网安全防护体系，技术具有独创性。

4、工

面向工业控制系统安全的定量评估和全生命周期防护技术

该技术是公司围绕国内火电、核电、冶金、石化的工业安全现状，在现有安全防护技术的基础上，提出的一种被动防御与主动防御相结合的安全防护技术。针对工控系统攻击机理和系统架构与业务特征，实现了覆盖工控系统各层级、全业务流程的异常检测，以及对工控系统未知威胁的主动发现，解决了跨越信息物理空间未知威胁的检测难题。该技术在线实时测评技术框架，综合考虑了各种度量因子，突破了工控安全难以度量、评估的技术瓶颈，在安全防护体系和主动防御理念方面均具有先进性，能够深度解析超过30种私有工控协议，提取300种以上主要的工业控制系统网络协议功能码，在理想状态下单个扫描任务速率达到每秒160万包，相关技术正在申请国家专利，已达到国内领先水平。

八、行稳致远，做美好未来的缔造者

慈善事业是社会建设的重要内容，是弘扬社会主义核心价值观的重要载体，对保障和改善民生，促进社会和谐稳定，推动社会文明进步都具有重要意义。

安恒信息作为一家具有高度社会责任感起家的企业，网络安保的基因伴随成长，“责任至上”已成为安恒的核心价值观之一。

1、 守护祖国网络疆土

“没有网络安全就没有国家安全”。安恒信息作为国家重大活动网络安全核心保障力量，拥有一支世界级网络安全保障团队，自2008年至今，共参与近百场国家重大活动的网络安全保障，圆满完成成为北京奥运会、上海世博会、历届世界互联网大会、G20杭州峰会、厦门金砖峰会、博鳌亚洲论坛、上合组织青岛峰会、武汉军运会等众多重大活动提供网络信息安全保障，并多次承担安保组长、安保中坚力量的职责，确保网络安保工作万无一失。

2、精准扶贫

2020年，公司积极响应国家关于脱贫攻坚工作的号召，以实际行动践行社会责任，积极投入到扶贫等公益事业中，参与并稳步推进相关多个扶贫项目，并实现当年落实完成。2020年公司完成的精准扶贫项目主要有以下几项：（1）2020年上半年，公司继续积极响应国家

关于脱贫攻坚工作的号召，以实际行动践行社会责任，积极投入到扶贫等公益事业中，为普安县和喜德县巴久乡捐款合计十一万元，助力两地产业发展。

(2) 安恒信息捐资助建的“蒲城县孝通小学安恒图书室”正式揭牌。

该项目旨在关注蒲城县青少年健康成长，普及网络安全知识。

(3) 教育信息化是推进精准扶贫脱贫的重要途径。公司努力落实教育信息化 2.0 行动计划中网络扶智工程攻坚行动，与教育部科技司合作，针对全国经济欠发达地区，展开线上网络安全职业培训。

3、人才培养

高校是我国培养网络空间安全人才的主阵地，网络空间的竞争，归根到底是人才的竞争，安恒信息通过竞赛的方式提升学生攻防兼备的网络创新实践能力，培养学生的创新意识与团队合作精神，普及信息安全知识，增强学生信息安全意识，提高学生的网络空间安全创新能力与实践技能。实现以赛促学、以赛促用，推动网络空间安全生态体系的人才培养和产学研用，安恒信息已连续多年为全国大学生信息安全竞赛提供技术支持。

与此同时，安恒信息与公安部三所、中国信息安全测评中心、中国网络安全审查技术与认证中心等部委、机构合作，共同提升我国网络安全治理水平和网络安全人才的综合技能水平，为国家发展和社会经济建设培养各层次网络安全人才。

4、关爱青少年

安恒信息建有省内第一个网络安全的科普教育基地。积极探索科普宣传的新思路、新方法、新手段，面向公众开放，积极开展科普活动，充分发挥科普教育基地在普及科学知识、倡导科学方法、传播科学思想、弘扬科学精神方面的作用，为进一步提升我省公众科学素质作出贡献。目前，已和 20 余家高校合作建立网络安全实验基地，在校园中开展网络安全普及教育活动，通过教学与实验相结合的方式，提高在校大学生的网络安全知识和防护能力，获得了在校师生极大的好评。

5、抗击疫情

面对“新型冠状病毒”疫情的挑战，安恒信息积极响应启动多项捐赠帮扶措施合力抗击疫情。

支援“火神山”医院，排查网络安全风险，提供网络安全防护能力

安恒密盾护航钉钉，1000 万中小企业在家办公信息安全无忧

安恒“堡垒机”免费开放远程办公安全运维服务，全力保障远程运维安全

公益保险计划，保障企业不受“信息疫情”

全面开放 X 平台在线学习资料，防疫期间提供“精神食粮”

对疫情重灾区求职者开辟绿色通道，为全国合作伙伴提供帮扶措施

安恒党委积极发挥红色堡垒作用，组建志愿者队伍，号召安恒党员和网络安保工程师加入，在疫情期间为武汉及全国多个地区提供技术支持服务。

捐赠上千台（套）网安设备

持续保障武汉与全国医疗机构网络安全

安恒党委牵头多渠道寻找医疗物资，持续捐赠驰援一线医疗机构
员工与企业捐款百万至湖北省，助力武汉共同抗疫