CSA GCR cloud security alliance
GREATER CHINA REGION ®

云安全联盟大中华区
2022年度研究成果合集精选

2023年4月

目 录

4.2 零信任

4.3 数据安全

4.4 物联网

4.5 区块链

4.6 个人信息保护

前言

数字经济在重组全球要素资源、重塑全球经济结构、改变全球竞争格局中起到关键作用，随之而来的是日益增加的安全风险。

如何保障云计算和数字化转型的安全性、合规性和可信性，是我们面临的共同课题。云安全联盟CSA作为世界领先的独立、权威国际产业组织，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识和全面发展。

为了促进数字安全技术的传播和交流，CSA每年都会发布一系列高质量的研究成果，涵盖了云安全、零信任、数据安全、物联网、区块链、隐私保护等多个领域。这些研究成果不仅反映了CSA在推动数字安全标准制定和实施方面的领导力，也展示了CSA在探索新兴技术应用和创新方案方面的前瞻性。

本合集精选了2022年度CSA发布的部分重要研究成果，包括技术标准、前沿产业报告和案例集。这些研究成果和落地案例既有理论深度又有实践指导意义，既有国际视野又有本土特色。我们希望通过本合集能够为广大读者提供一个系统而全面的数字安全知识体系，帮助读者掌握最新的数字安全趋势和技术，并应用到自身的工作场景中。

我们衷心感谢所有参与本合集编写和审阅工作的专家学者、企业代表以及CSA团队成员，他们付出了大量的时间和精力，确保本合集内容质量。同时，我们也欢迎读者对本合集提出宝贵意见或建议，并期待与读者在未来继续交流学习。

致谢

感谢以下人员对CSA大中华区2022年研究工作的支持（排名不分先后）：

艾龙、安涛、毕立波、毕亲波、毕月乌、卞乐彬、岑义涛、曾令平、曾永红、柴瑶琳、常向青、车洵、陈本峰、陈丑亚、陈冠直、陈皓、陈俊杰、陈龙、陈强、陈吴栋、陈欣炜、陈妍、陈钟、程伟强、仇俊杰、仇蓉蓉、崔灏、崔崟、戴才良、戴立伟、单美晨、邓辉、丁俊贤、丁哲轩、董明富、董天宇、董雁超、方婷、方伟、伏伟任、付艳艳、付宗玉、高瑞强、高巍、高亚楠、高卓、葛岱斌、顾立明、顾伟、郭春梅、郭海骏、郭嘉伟、韩淑君、韩小平、郝振武、何国锋、何维兵、何伊圣、何艺、贺进、贺志生、洪重良、侯汉书、侯俊、胡钢伟、胡向亮、黄超、黄晖、黄连金、黄鹏华、黄瑞、黄妍昕、计东、季文东、贾玉彬、江坤、江楠、江澎、江泽鑫、姜国春、姜宁、姜政伟、蒋秋华、蒋蓉生、蒋晓、解佳、靳倩倩、寇翔淋、乐元、雷钰婷、黎伊帆、李安伦、李滨、李博、李国、李洪雨、李吉祥、李娇娇、李金瑞、李来冰、李钠、李娜容、李沈舟、李帅宇、李腾飞、李鑫、李岩、李奕纬、梁小毅、廖武锋、廖振勇、林冠烨、林艺芳、刘斌、刘博、刘楚楚、刘芳、刘广坤、刘国强、刘洪森、刘洁、刘隽良、刘涛、刘文懋、刘旭、刘雅梅、刘宇馨、刘玉红、刘志诚、卢佐华、陆建松、陆琪、陆琦玮、鹿淑煜、罗川、罗春、罗进、罗晓兰、吕士表、马超、马嘉、马琳琳、马权、马维士、马晓艳、毛备、茆正华、穆域博、欧建军、潘盛合、潘万鹏、潘义华、秦柯、秦益飞、邱勤、任亮、任永攀、申屠鹏会、沈勇、石瑞生、时培宇、史宇航、宋平、苏泰泉、汤霖、陶瑞岩、滕伟、田原、童磊、汪海、王安宇、王彪、王贵宗、王辉、王良河、王亮、王娜、王其勇、王茜、王伟、王玮、王岩、王扬、王阳、王永霞、王雨萌、王泽、魏超、魏东、魏小强、文慧智、文黎力、吴贺、吴嘉雯、吴满、吴湘宁、吴潇、吴欣、夏永涛、肖达、谢佳、谢江、谢琴、谢泳、邢海韬、徐帅健妮、徐文想、徐岩、薛恺、薛琨、闫新成、严东、杨洪起、杨岁立、杨天识、杨文宏、杨喜龙、杨学治、杨玉欢、杨育斌、杨震东、杨正权、杨志刚、殷铭、于继万、于乐、于新宇、余其玄、余强、余滔、余晓光、俞华辰、袁明坤、袁荣婷、袁淑美、袁帅、原浩、岳炳词、岳婧、张彬、张兵、张超、张光治、张建盛、张亮、张淼、张明敏、张睿、张赛楠、张涛、张晓华、张元恺、张钊、赵晨明、赵睿、赵帅、赵仰梅、赵晔、赵勇智、赵宇、郑斌、郑剑锋、郑宁、郑亚东、钟施仪、周海生、周杰、周利斌、周溥璇、周星宇、周轩立、周泽元、周智坚、朱梦婷、左奕航

致谢

感谢以下单位对CSA大中华区2022年研究工作的支持（排名不分先后）：

Fortinet（飞塔）、OPPO、阿里、安恒、安几网安、安全狗、安信与诚 、安讯奔 、安易科技 、奥创科技 、白山云 、北森 、持安科技 、迪普科技 、缔安科技 、格尔软件 、谷安天下 、观安信息 、海尔 、虎符网络 、华为 、华云安 、吉大正元 、极氪 、江南天安 、浪潮云 、联软科技 、绿盟科技 、美创 、美云智数 、魔方安全 、派拉软件 、奇安信 、奇虎360 、360数科 、启明星辰 、青藤 、任子行 、赛宝认证 、赛虎网安 、三未信安 、山石网科 、上海CA 、深信服 、深圳国家金融科技测评中心 、神州数码 、世平信息 、数安行 、顺丰科技 、碳泽 、腾讯 、E签宝 、天融信 、天翼安全 、网宿科技 、网御星云 、威联科技 、微步在线 、物盾信息 、小佑科技 、芯盾时代 、新华三 、信通院 、兴业数金 、亿格云 、易安联 、熠数信息 、云山雾隐 、云深互联 、浙江大华 、智安网络 、智慧云测 、中孚信息 、中国电信 、中国电信研究院 、中国工商银行 、中国移动 、中兴通讯 、中宇万通 、众人智能等联盟成员单位。

关于云安全联盟大中华区

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

联盟宗旨

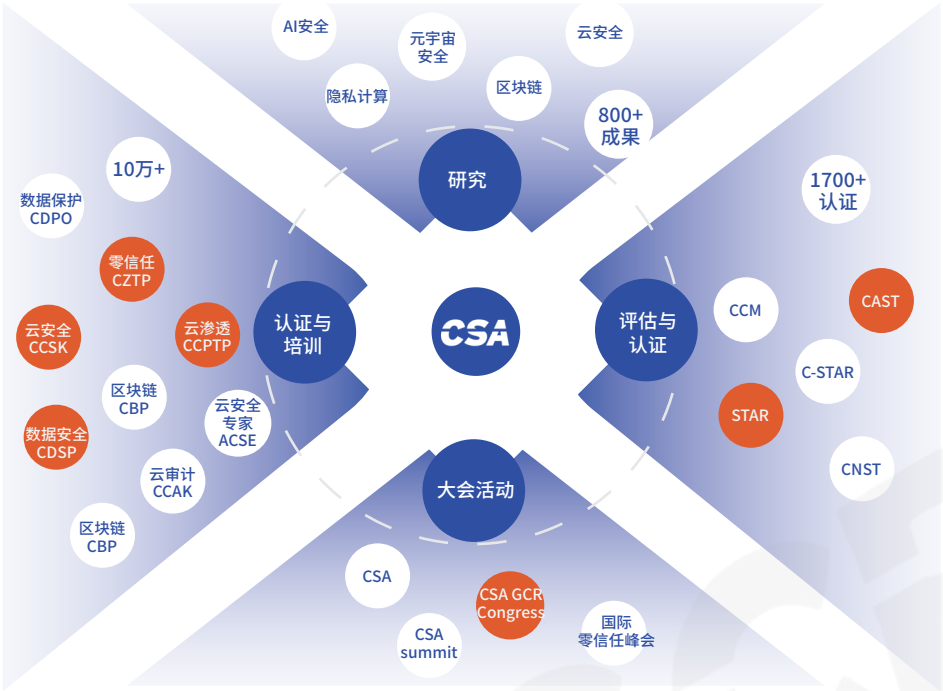
推动业界对云安全与数字安全的前沿研究；

推广正确使用云安全及数字安全的解决方案，和开展教育计划；

帮助个人、企业用户和供应商达到要求的安全认识水平与能力，并提供安全认证证书。

CSA全球布局

CSA在全球设立四大区，包括美洲区、欧非区、亚太区和大中华区，100多支分会覆盖50多个国家，1000多家会员单位，15万多社区专业从业人员。



企业会员

目前CSA企业会员已有1500+家，覆盖数据安全、零信任、隐私计算、云安全、人工智能等各个技术领域，企业类型包括世界500强科技公司、多数网络安全上市公司或独角兽公司、云服务商、云或安全用户、以及初创企业等。

CSA全球高级执行会员(部分)

CROWDSTRIKE　DTCC　Google　HUAWEI　IBM Security　Microsoft　netskope

okta　OneTrust　ORACLE CLOUD　Qualys.　WiZ

CSA 全球会员(部分)

CAICT 中国信息通信研究院　中国检验认证集团检验有限公司　国家金融科技测评中心　赛宝认证中心　阿里云　腾讯云　ZTE中兴

oppo　360　SANGFOR 深信服科技　奇安信　inspur 浪潮　sansec 三未信安　amazon web services

CISCO　DELL Technologies　Deloitte.　EY Building a better working world　pwc　ebay　GitHub

PayPal　McAfee　APPGATE　Bell　ExtraHop Rise Above the Noise.　paloalto NETWORKS　FORTINET

CSA大中华区理事单位(部分)

CSA大中华区会员单位(部分)

加入我们

成为CSA企业会员或专家会员，共同致力于云安全与下一代数字技术安全的全面发展。

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

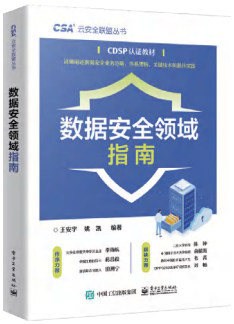
了解联盟更多信息，请
扫码下载联盟会刊手册

JOIN US

更多联系：
CSA大中华区常务副秘书长 许女士 18218024060 melanxu@c-csa.cn
CSA大中华区办公室主任 叶女士 19925407556 candyye@c-csa.cn

云安全联盟丛书

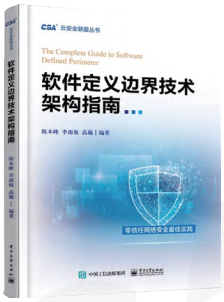
丛书的编写将坚持理论与实践并重的原则，既保证理论知识的准确严谨，又注重实践方案的价值落地。丛书内容将涵盖云安全、大数据安全、物联网安全、零信任安全、5G安全、人工智能安全和区块链安全等新兴技术领域安全。本丛书既可用于CSA认证课程学习教材、高等院校和社会教育所用教材或教学参考书，也可以作为产业界的专业安全读物。



CSA云安全联盟丛书

《数据安全领域指南》

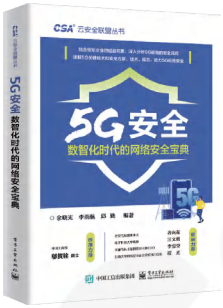
《数据安全领域指南》购书优惠码



CSA云安全联盟丛书

《软件定义边界技术架构指南》

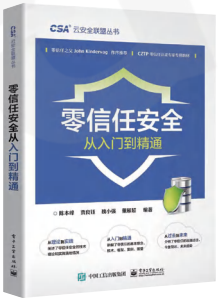
《软件定义边界技术架构指南》购书优惠码



CSA云安全联盟丛书

《5G安全》

《5G安全》购书优惠码



CSA云安全联盟丛书

《零信任安全从入门到精通》

敬请期待

云渗透测试认证专家CCPTP

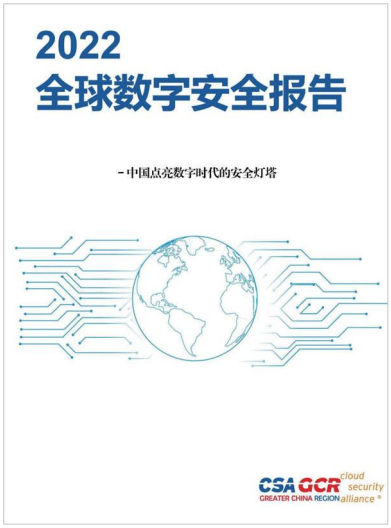
云渗透测试认证专家（Certified Cloud Penetration Test Professional, CCPTP）认证与培训项目由国际云安全联盟中华区发布，是全球首个针对云环境渗透测试能力的认证课程，旨在提供针对云计算渗透测试所需的专业实操技能，弥补云渗透测试认知的差距和技能人才培养的空白，提升专业人员能力及提供认证证书，为云计算产业发展提供渗透人才队伍保障。

CCPTP®
Certified
Cloud Penetration Test Professional

认证课程包含了云渗透测试体系、测试流程、实践技术、法律法规、渗透测试人员道德规范、渗透测试方法论以及实操技术等内容。通过CCPTP的考试，确保从事云计算及渗透测试相关的安全从业人员对云渗透测试体系架构、法律法规、测试技术以及实践技术有一个全面的了解和广泛的认知，帮助云安全专业人员深入了解云上渗透　测试工作，以便在客户授权的前提下进行渗透测试及合法地评估目标系统的安全状态，并为解决云安全问题提供帮助。

CCPTP证书模板

1 《全球数字安全报告》



随着数字经济、数字政府、数字社会等的快速发展，我们正处于数字时代。数字技术和数据不仅带来了新的理念、机遇和好处，也给所有国家带来了挑战、威胁和风险。消费者的数据安全和隐私保护已经从线下转移到线上，海量数据也引发了数个数据安全管理问题。随着数字技术为社会经济服务的范围和深度越来越大，安全问题的后果将更加严重。面对日益增加的安全风险，没有人可以单打独斗。数字安全不是单纯的技术问题，而是涉及业务、管理、流程、团队等多方面的系统工程。数字经济高质量发展涉及政策、法律、技术等多方面的协同配合。需要构建原生安全能力，以数字安全和可信为基础。

世界各国都在不断优化数据安全政策。欧盟发布的《欧洲数据保护监管局战略计划（2020-2024）》继续加强数据安全和个人隐私保护。美国发布《2020年联邦数据战略和行动计划》，确立了保护数据完整性、确保流通数据真实性、数据存储安全等基本原则。《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》也于2021年颁布。本文档基于 CSA大中华区提出的数字安全REE框架，调研了全球数字安全各领域的现状，并总结了优先的实践、流行的技术，和公认的数字安全提供商，还包括全球重要的法律、法规、标准，向读者介绍数字安全的发展概况，特别是中国的状况。希望该文件能成为政府与行业在数字安全方面的参考，帮助人们构建更加安全的数字环境。

扫描公众号二维码，回复“安全报告”，获取完整报告

2

案例集

2.1 CSA 2022年度企业奖项获奖案例

CSA 2022安全磐石奖

表彰该单位的解决方案综合性强，在方案思路和技术应用方面具备创新亮点，能够有效解决企业或用户在新型网络环境中的数字安全问题，可以为业内提供良好的参考价值及引领作用。

序号	单位名称	解决方案名称
1	华为软件技术有限公司	华为终端云安全解决方案
2	浪潮云信息技术股份公司	数字政府安全运营支撑体系建设方案
3	北京神州绿盟科技有限公司	T-ONE CLOUD
4	奇安信科技集团股份有限公司	冬奥网络安全“零事故”解决方案
5	深信服科技股份有限公司	XDR可扩展检测响应解决方案
6	阿里云计算有限公司	零信任安全——办公安全平台SASE
7	北京奇虎科技有限公司	360企业安全云
8	启明星辰信息技术集团股份有限公司	安全算力网络解决方案
9	格尔软件股份有限公司	政务云密码服务平台解决方案
10	新华三技术有限公司	工业互联网安全解决方案
11	亚信安全科技股份有限公司	终端零信任解决方案
12	杭州安恒信息技术股份有限公司	工业互联网安全综合服务平台解决方案
13	中移（苏州）软件技术有限公司	政企云安全综合解决方案
14	浙江大华技术股份有限公司	AI数据与隐私保护方案 —巨灵AI开放平台

扫描公众号二维码，回复“案例集”，获取企业案例

CSA 2022安全金盾奖

表彰该单位的安全解决方案/产品或安全服务具备核心竞争力，能够解决当前行业领域亟需解决的主要问题，在相关领域占据重要的市场份额，该单位的产品方案或安全服务被众多单位采用，且具备一定创新性，并得到业界认可，是相关安全领域的佼佼者。

序号	单位名称	解决方案名称
1	北京火山引擎科技有限公司	容器安全防护平台产品
2	北京神州数码云计算有限公司	数据安全管控平台
3	联通（上海）产业互联网有限公司	云盾抗 D 先锋
4	腾讯云计算（北京）有限责任公司	云访问安全代理CASB
5	中孚信息股份有限公司	数据安全交换系统
6	深圳市联软科技股份有限公司	全网零信任安全管理解决方案
7	天融信科技集团股份有限公司	零信任远程办公安全解决方案
8	浙江齐安信息科技有限公司	检修作业安全运维系统
9	北京指掌易科技有限公司	灵犀·零信任SDP安全网关
10	杭州盈高科技有限公司	ASM入网规范管理系统
11	杭州美创科技股份有限公司	数据库防水坝系统
12	三未信安科技股份有限公司	数据加密服务
13	北京持安科技有限公司	持安远望办公安全平台
14	北京蔷薇灵动科技有限公司	蜂巢自适应微隔离安全平台
15	江苏易安联网络技术有限公司	零信任安全解决方案
16	江苏保旺达软件技术有限公司	合规和安全双驱动的方舟数据安全管控平台
17	北京芯盾时代科技有限公司	零信任业务安全平台
18	厦门服云信息科技有限公司	云甲·云原生容器安全管理系统
19	贵州白山云科技股份有限公司	ACCESS应用可信访问
20	长春吉大正元信息技术股份有限公司	数字证书认证系统
21	北京小佑网络科技有限公司	镜界云原生容器安全检测平台

扫描公众号二维码，回复“案例集”，获取企业案例

CSA 2022安全创新奖

表彰该单位在数字安全及各项新兴技术领域方向有创新的安全产品、新颖的解决方案，解决了行业当前关键的疑难问题，其关键技术指标达到国内外领先水平，为数字安全行业的发展提供新的思想和技术创新，能够实现产业化发展落地。

序号	单位名称	序号	单位名称
1	杭州锘崴信息科技有限公司	2	上海观安信息技术股份有限公司
3	杭州默安科技有限公司	4	中国电信股份有限公司上海研究院
5	杭州极盾数字科技有限公司	6	北京安讯奔科技有限责任公司
7	鼎特（北京）信息技术有限公司	8	深圳市智安网络有限公司
9	北京江南天安科技有限公司	10	深圳市魔方安全科技有限公司
11	北京华云安信息技术有限公司	12	北京数安行科技有限公司
13	上海安几科技有限公司	14	上海碳泽信息科技有限公司
15	上海物盾信息科技有限公司	16	杭州孝道科技有限公司
17	上海派拉软件股份有限公司	19	深圳国家金融科技测评中心有限公司
19	杭州世平信息科技有限公司	20	北京从云科技有限公司
21	苏州云至深技术有限公司		

CSA 2022革新奖

表彰该单位积极创新，勇于接纳数字安全新技术和新范式，自我革新，提升数字安全能力，整体建设处于行业领先地位，在业界有较好的声誉和影响力，是同领域其他企业数字安全建设的风向标。

序号	单位名称	序号	单位名称
1	中兴通讯股份有限公司	2	新东方教育科技集团
3	杭州市拱墅区数据资源管理局	4	顺丰控股股份有限公司
5	兴业银行股份有限公司漳州分行	6	深圳乐信软件技术有限公司
7	上海东普信息科技有限公司	8	杭州天谷信息科技有限公司
9	中国大地财产保险股份有限公司		

扫描公众号二维码，回复“案例集”，获取企业案例

CSA 2022数字化转型安全支撑案例 2.2

CSA 数字化转型安全支撑案例 TOP 10

序号	案例名称	单位名称
1	光大银行全栈云容器平台安全防护建设实践	北京小佑网络科技有限公司
2	青藤蜂巢·云原生安全平台	青藤云安全
3	金融企业基于微隔离的数据中心零信任建设实践	北京蔷薇灵动科技有限公司
4	民生银行企业应用移动化零信任体系建设项目	中国民生银行
5	业权一体化护航企业数字化转型	广东美云智数科技有限公司
6	安恒信息AiLand数据安全岛数据要素流通实践	杭州安恒信息技术股份有限公司
7	移动应用全生命周期管理平台	中国电信股份有限公司上海研究院
8	四川阿坝州政务云平台安全实践	北京天融信网络安全技术有限公司
9	绿盟科技构建安全底座，护航数字西青	北京神州绿盟科技有限公司
10	腾讯iOA助力贝壳找房落地零信任安全战略	腾讯云计算（北京）有限责任公司

CSA 数字化转型安全支撑优秀案例

序号	案例名称	单位名称
1	竹叶青茶业基于零信任的综合安全防护体系	成都云山雾隐科技有限公司
2	国家电网安全体系威胁情报综合应用案例	北京微步在线科技有限公司
3	某某云全网漏洞监测管理与预警落地案例	北京华云安信息技术有限公司
4	千乘SOAR安全编排与响应平台金融实践案例	上海碳泽信息科技有限公司
5	某证券交易所基于人工智能的高级威胁检测项目实践	北京金睛云华科技有限公司
6	零信任数据安全防护方案在大数据局的实践案例	杭州虎符网络有限公司
7	基于电力物联网综合示范园区的零信任网络安全防护体系	杭州漠坦尼科技有限公司
8	危化安全生产数字化（区块链）监管平台	杭州宇链科技有限公司
9	阳光保险集团养老与不动产中心零信任落地案例	云深互联（北京）科技有限公司
10	宁盾一体化身份与访问管理平台	上海宁盾信息科技有限公司
11	浙江吉利控股集团资产风险检测管理平台建设	杭州默安科技有限公司
12	物联网安全运营中心	北京方研矩行科技有限公司
13	台州市大数据局“公共数据平台”数据安全建设实践	杭州美创科技有限公司
14	中国石化统一身份管理系统	石化盈科信息技术有限责任公司
15	构建统一电子签章平台，赋能地产企业数字化转型	北京数字认证股份有限公司

扫描公众号二维码，回复“案例集”，获取企业案例

2.3 CSA 2021零信任落地案例集

序号	案例所属行业	零信任技术	案例用户名称	案例用户名称
1	政企	SDP	温州市大数据发展管理局	安恒信息
2	政企	SDP	某市海事局	任子行
3	政企	SDP	部委大数据中心（2020 年案例）	奇安信
4	政企	IAM	某大型集团公司	吉大正元
5	政企	SDP	中国航空工业集团有限公司	格尔软件
6	政企	微隔离	招商局集团	厦门服云
7	交通	SDP	山东港口集团	深信服
8	能源	SDP	某省电力公司直属单位	漠坦尼
9	能源	SDP	中国核工业华兴建设有限公司	易安联
10	能源	SDP	国家电网有限公司某二级直属单位	虎符网络
11	金融	SDP	某大型商业银行	奇安信
12	金融	微隔离	中国交通建设股份有限公司	薔薇灵动
13	金融	SDP	中国建设银行	缔盟云
14	金融	SDP	光大银行	联软
15	金融	SDP	阳光保险集团养老与不动产中心	云深互联
16	互联网	SDP	贵州白山云科技股份有限公司	上海云盾
17	互联网	IAM	E 签宝	天谷信息
18	运营商	SDP,IAM	电信运营商	芯盾时代
19	运营商	SDP	电信运营商	云深互联

扫描公众号二维码，回复“案例集”，获取企业案例

3

技术标准

《云应用安全技术规范》

《云应用安全技术规范》确立云应用产品应该具备的安全相关的技术或能力要求。云应用包括但不限于SaaS云应用、PaaS和IaaS云的应用程序部分。云应用提供服务的形式可以是web应用、移动APP、API接口等。


CSA 云安全联盟标准

CSA GCR C001—2022

云应用安全技术规范

Cloud Application Security Technology Specification

2022－03－09 发布

云安全联盟大中华区 发布

该规范为云应用厂商或甲方构建安全的云应用产品提供参考和指导，为云客户选择安全的云应用产品提供参考和指南。

该规范对云应用应该具备的安全技术或能力要求进行了说明，主要包括云应用架构设计要求、云应用运行环境安全要求、云应用程序安全要求、访问控制安全要求、租户级安全自助能力要求、云实施/交付/服务安全要求、云数据安全要求、云安全管理能力要求共8个控制域，各控制域包含的主要控制项如下图所示。

云应用安全框架

扫描公众号二维码，回复“技术标准”，获取完整报告

《云原生安全技术规范》


CSA GCR C002—2022

CSA 云安全联盟标准

CSA GCR C002—2022

云原生安全技术规范

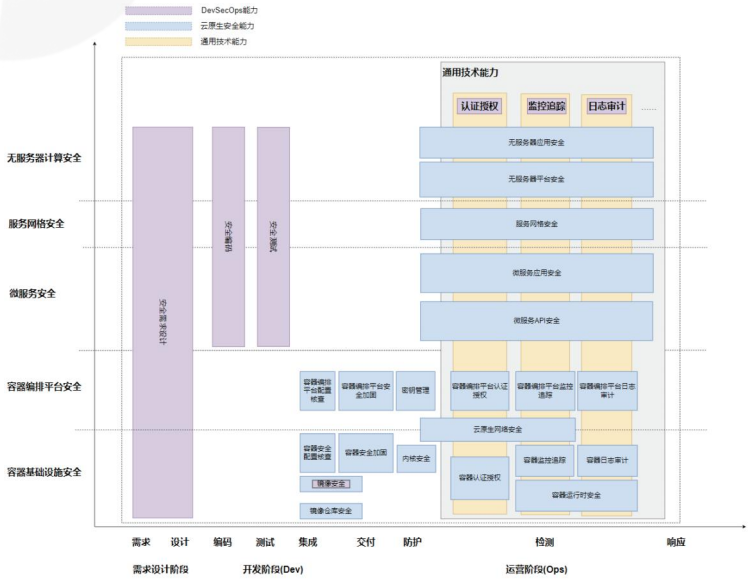
Cloud Native Security Technology Specification

2022－05－05 发布

云安全联盟大中华区　　发布

《云原生安全技术规范》针对云原生安全体系中涉及的每类技术制定的标准。该规范适用于为云原生类产品厂商或甲方构建安全的云原生类产品提供参考和指导。

下图描述了前述的云原生安全框架。其中，横轴是开发运营安全维度，涉需求设计（Plan）、开发（Dev）、运营阶段（Ops），细分为需求、设计、编码、测试、集成、交付、防护、检测、响应阶段，但考虑到响应安全能力要求在不同云原生技术层差异性较大，本标准不涉及响应阶段：而纵轴则是按照云原生系统和技术的层次划分，包括容器基础设施安全、容器编排平台安全、微服务安全、服务网格安全、无服务器计算安全五个部分。其中，从云原生安全的视角，云原生 IT 系统各层所需的安全要求从容器基础设施安全、容器编排系统安全，直至无服务器计算安全，对应图中蓝色标注部分。纵轴则是按照云原生系统和技术的层次划分 包括容器基础设施安全、容器编排平台安全、微服务安全、服务网格安全 、无服务器计算安全五部分。



云原生安全体系框架

扫描公众号二维码，回复“技术标准”，获取完整报告

《物联网安全规范》

本文件给出了物联网系统应该具备的安全相关的技术或能力要求，规定了物联网安全对象及各相关方的安全责任。本文件提供各应用工业物联网领域的设备厂商或甲方构建安全的物联网系统的指导，也可为各组织制定自身的物联网安全标准提供参考。

物联网安全技术框架主要是在合法合规的基础上，通过安全治理、物联网系统安全防护、运营和运维以及安全开发来进行设计；法律法规的遵从主要是通过对法律合规进行评估，并落实实施计划和制定相关文件；安全治理主要通过分析物联网所特有的安全需求，提出有针对性的安全策略方针，从而形成适用于物联网业务的安全治理方案；物联网系统安全防护主要从物理层、设备层、网络层、应用层展开设计；安全运营和运维描述了安全控制的具体技术实现；安全开发主要通过对整个开发流程的安全措施和策略、供应链安全及安全测试的实施来保障。

物联网安全技术框架结构

扫描公众号二维码，回复“技术标准”，获取完整报告

《软件定义边界（SDP）标准规范2.0》

SDP为网络运营者提供动态灵活的边界功能部署能力，聚焦于保护关键的组织资产，可实现精准授权，降低网络攻击的可能性。SDP是零信任原则不可分割的一部分，它帮助零信任安全实现最小授权原则，隐蔽网络和资源。信息安全是动态发展的，新技术不断推陈出新，SDP就是在传统的技术生态中迭代形成的一套技术架构，它是多种网络安全技术的整合，包括密码技术、网络技术、访问控制技术和软件开发技术等，SDP适用场景也非常广泛，包括云计算、物联网、大数据、工业互联网、移动互联网等，为SDP体系架构的发展提供了更多的可能。　在“后疫情时代”的背景下，网络资源快速开发和利用，远程办公、线上教育、勒索病毒、网络攻击、网络诈骗等对我们管理能力提出了严峻挑战，面对网络环境的复杂变化，SDP2.0体系的应用将为网络空间的健康发展起到重要的支撑作用。本规范通过通俗易懂的语言向大家介绍了SDP2.0的体系架构、部署模型、访问流程等，希望你在读完本规范后可对SDP有更为清晰的理解，并帮助你更快完成应用实践。

扫描公众号二维码，回复“技术标准”，获取完整报告

4

产业报告

《面向云客户的SaaS治理最佳实践》

报告背景

据 Statista 预测，到 2022 年全球企业服务 Saas 市场规模将超 1700 亿美元，Saa 成了真正的“软件终结者”。国内 Saas 虽然起步较晚但也已经在 2019 年进入了旺盛期，CRM、ERP、HCM、OA、财务、客服、电子签名等垂直领域的 Saas 蓬勃发展。传统软件厂商也纷纷向 Saas 转型。尤其是新冠疫情暴发以来，很多企业不得不选择远程办公和使用线上 Saas 应用，疫情成为 Saas 发展强有力的助推剂。

报告概述

随着 Saas 的普及，企业软件的安全风险从传统软件转移到了 SaaS 应用。企业的云安全治理范围也从原来的 laas 基础设施层和 Paas 平台层延伸到了 SaaS 应用层。因此，CSA 在发布 CAST 云应用安全可信标准与认证之后，又发布了《面向云客户的 SaaS 治理最佳实践》（以下简称《实践》）白皮书，供SaaS 从业人员及相关的 T 或安全从业人员参考。《实践》充分关注到了 Saas 环境中的数据保护、Saas 生命周期的风险以及处置等内容。而且基于安全策略、安全组织、资产管理、访问控制、加密和密钥管理、安全运维、网络安全、供应商管理、事件管理、合规等多个安全控制域为业界提供一整套用于 Saas 治理的指南。《实践》围绕 SaaS 治理中最核心的问题“确保谁在什么场景下、拥有什么样的权限、可以访问什么数据”，并从评估、采用、使用和终止四个阶段给出了具体措施和建设，同时针对日常应用场景进行了延伸的安全考量。

适宜读者

SaaS.客户、Saas.客户、SaaS云服务提供商、SaaS 安全解决方案提供商、云安全专业人员、法务、网络安全主管、IT 主管、风险经理、IT 审计员和合规人员、第三方风险经理。

扫描公众号二维码，回复“云安全”，获取完整报告

《云计算的 11 类顶级威胁》

报告背景

如今，越来越多的企业正在将数据和应用程序迁移到云中，这带来了独特的信息安全挑战。而企业在使用云计算服务时将面临 11 个主要的云安全威胁。保护企业在云中数据的主要责任并完全不在于服务提供商，而主要在于客户本身。为了使组织对云安全问题有新的了解，以便他们可以就云采用策略做出有根据的决策，云安全联盟CSA发布了新版本的《云计算的 11 类顶级威胁》，报告反映了 CSA 安全专家之间当前就云中重要的安全问题达成的共识。

报告概述

“顶级威胁”报告一贯旨在提高对云平台威胁，风险和漏洞的认识。此类问题通常由云计算按需和共享的天生特征导致。在第四部分中，我们再次就云行业安全问题与241位行业专家进行调查。今年，我们的受访者对其云环境中的11 个主要威胁，风险和漏洞进行了评估。最高威胁工作组结合调查结果及专业知识来撰写2019 年最终报告。

最新报告按调查结果重要程度着重介绍了前 11 个威胁（括号中是以往的排名）：

1.数据泄露、2.配置错误和变更控制不足、3.缺乏云安全架构和策略、4.身份，凭证，访问和密钥管理不足、5.账户劫持、6.内部威胁、7.不安全的接口和 API、8.控制平面薄弱、9.元结构和应用程序结构失效、10.有限的云使用可见性、11.滥用及违法使用云服务

适宜读者

基于行业从业者、协会、政府，以及企业和个人会员、安全专家、云安全研究、教育、认证、活动者，组织以及云供应商。

扫描公众号二维码，回复“云安全”，获取完整报告

《微服务架构模式》

报告背景

随着数字化时代的到来，微服务应用进入飞速发展时代。微服务是一种新兴的分布式系统开发范式，在架构层面，安全性是必须认真考虑的重要工作。我国随着《数据安全法》和《个人信息保护法》的颁布，对安全和数据保护的重视程度日益提高，架构层的安全问题必将上升到组织安全治理层面

报告概述

如何保证微服务架构的安全？本文档给出了 CSA 的最佳实践与总结，通过 CSA 微服务安全参考架构以及安全控制措施叠加的新思路，保证了微服务在架构层面的安全性，CSA 微服务安全工作组也在陆续推出微服务安全相关的指南与白皮书，文章深入浅出，值得大家参考。制措施叠加的新思路，保证了微服务在架构层面的安全性，CSA 微服务安全工作组也在陆续推出微服务安全相关的指南与白皮书，文章深入浅出，值得大家参考。

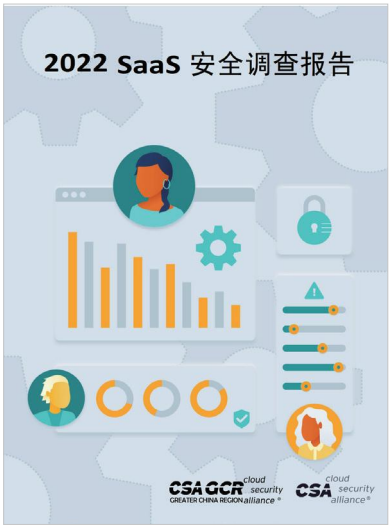
本文旨在提出一种可重复的方法，用于按“MAP”(Microservices Architecture Pattern.微服务架构模式）构建、开发和部署微服务。我们提出的这个“MAP”包含微服务独立运行和与其他微服务通信所需要的全部信息——这些微服务聚合到一起，会形成转而又会成为应用程序成分的能力。本文描述了“MAP”的关键元素、应该怎样设计和部署，以及应该怎样通过一种合规即代码方法把安全和合规左移。本文的主要目的是开发一个厂商中性的参考架构基础，从这个基础分解出软件和平台（企业）平面体现的软件架构模式，以后还可以通过添加安全控制措施叠加重新构建。微服务架构模式的成功分解和重组就证明了这一点，其中的集成操作便是安全控制措施的叠加。

适宜读者

应用程序开发人员、应用程序架构师、系统和安全管理员、安全项目经理、信息系统安全官以及其他对应用程序容器和微服务的安全负有责任或感兴趣的人员。

扫描公众号二维码，回复“云安全”，获取完整报告

《2022 SaaS 安全调查报告》



报告背景

从Salesforce 1999年发布CRM SaaS 服务成为SaaS的开拓者，到2022年全球企业服务SaaS市场规模将超1700亿美元（据Statista预测），SaaS成了真正的“软件终结者”。国内SaaS虽然起步较晚但也已经在2019年进入了旺盛期，CRM、ERP、HCM、OA、财务、客服、电子签等垂直领域的SaaS蓬勃发展。而且几乎所有传统的管理软件企业都开始了新一轮的转型尝试。

报告概述

许多最近发生的违规与数据泄露事件由错误配置导致，多数关于错误配置的研究只关注IaaS层，而忽略了SaaS全栈。然而，SaaS安全和错误配置对于企业的整体安全同等重要。基于上述原因，CSA设计并发布了一项调查，以便更好地了解SaaS应用的使用，SaaS安全性评估的工具与时间表，检测和修复错误配置的时间表，以及对SaaS应用相关安全工具的认识了解。如何保证企业在日益复杂的网络环境下的数字安全，保证云上业务的安全？这些问题在《报告》中也给出了相对应的解决思路。除此之外，《报告》中的一些对比数据或许可以为企业解决SaaS安全问题提供借鉴，给企业的使用SaaS带来一些启示。对于很多企业来说，安全地使用SaaS是一个很有挑战的过程，需要加强企业内部的控制策略，并通过统一的安全保障措施和策略对SaaS应用进行识别和管控。同时推荐使用SSPM管理，为安全团队提供SaaS应用程序安全设置可见性的能力，也可以利用

适宜读者

SaaS.客户、Saas.客户、SaaS云服务提供商、SaaS 安全解决方案提供商、云安全专业人员、法务、网络安全主管、IT 主管、风险经理、IT 审计员和合规人员、第三方风险经理。

扫描公众号二维码，回复“云安全”，获取完整报告

《实现安全应用容器架构的最佳实践》

报告背景

在DevOps等一些敏捷软件开发方法的设计、开发和部署应用阶段往往会采用应用容器和微服务架构。这些软件开发方法里需要嵌入安全。本文从开发者、运营者和架构师的视角，提出了一些建议和最佳实践，解决在可信赖的安全系统工程中保护应用程序容器所面临的挑战。

报告概述

此次发布的《实现安全应用容器架构的最佳实践》充分考虑了这些年安全应用容器架构的技术发展和行业需求，更好地满足数字化安全的未来发展。如今，在DevOps等一些敏捷软件开发方法的设计、开发和部署应用阶段往往会采用应用容器和微服务架构。这些软件开发方法里需要嵌入安全。安全的DevOps要求安全人员、开发者和运营者协同工作，方可设计、构建出值得信赖的安全系统。

适宜读者

此文档面向应用开发者、应用架构师、系统和安全管理者、安全项目经理、信息系统安全官和其他相关责任人或对软件开发生命周期中的应用容器安全感兴趣的人员。

扫描公众号二维码，回复“云安全”，获取完整报告

《如何设计安全的无服务器架构》

报告背景

在当今快节奏的商业环境下，开发人员被要求更迅速地构建和部署应用程序以跟上业务发展需求，同时云原生理念也被普遍接受，基于云原生的无服务器架构因此日渐受到业界青睐。

报告概述

本文全面概括了无服务器平台的各种威胁，重点关注无服务器平台应用程序所有者面临的风险，聚焦于最佳实践，并提供了适当的安全控制建议。文中提出的基于无服务器平台应用程序所有者面临的风险，聚焦于最佳实践，并提供了适当的安全控制建议。文中提出的基于无服务器的安全计算执行模型，对指导应用程序所有者如何采用无服务器架构具有极好的参考价值。

适宜读者

本文主要适用于应用开发人员、应用架构师、安全专业人员、首席信息安全官（CISO）、风险管理专业人员、系统与安全管理员、安全项目经理、信息系统安全官以及任何对无服务器计算安全感兴趣的人。

扫描公众号二维码，回复“云安全”，获取完整报告

《云安全现状、挑战和安全事件》

报告背景

随着云计算等企业级技术应用的发展普及，产业互联网实际已经在各行各业展开实践。数据信息由此实现从消费端到供给端的高效流通，数字产业与传统产业相互协同带动，助推中国经济迈向高质量发展阶段。在新旧动能接续转换的过程中，传统产业的数字化升级和新兴产业的数字化能力建设，使当前的安全趋势发生了变化。该报告基于互联网、产业互联网及相关领域在上云过程当中面临的安全态势、风险趋势、应对力量以及监管状态等进行梳理，以期为行业提供阶段性的总结和建议，助力云上各方有策略地建立安全能力，更好应对安全风险。

报告概述

在过去的十年中，云服务的使用持续增长。CSA%20制定并分发了一项调查，以更好地了解当前的云安全的问题、挑战和事件。超过一半的企业在公共云中运行%2041%25或以上的工作负载，是自2019%20年以来的显著增长。2019%20年发现只有%2025%25的企业在公共云中运行%2041%25或更多的工作负载。2021%20年，63%25的受访者预计将在公共云中运行%2041%25或更多的工作负载，这表明这种公共云的发展趋势会持续进行。毫无疑问，由于最近的健康危机，远程工作者的增加将进一步起到推动作用。CSA在2020年进行的另一项调查也表明，生产工作负载的多样性（如容器平台、虚拟机）也将增加。

适宜读者

云计算管理员、云计算架构师、云计算安全经理、云应用开发人员、云计算软件工程师、基于行业从业者、协会、政府，以及企业和个人会员，安全专家，云安全研究、教育、认证、活动者，组织以及云供应商。

扫描公众号二维码，回复“云安全”，获取完整报告

《保护云中医疗健康数据的隐私》

报告背景

数字经济时代，医疗健康数据的开发利用有利于广大民众的健康生活，但同时作为一类特殊的隐私数据，患者、医生包括医疗机构等全产业链的数据安全面临着巨大的泄漏风险。如何保证云端的医疗健康数据尤其是敏感的隐私数据的安全，需要数据控制者和数据处理者从数据的全生命周期考虑安全，数据安全是数据治理的重要组成部分，在企业数字化转型中需要重点考虑。本白皮书结合业内最佳实践从隐私工程、风险评估、隐私监管几个方面阐述了云端医疗健康数据的保护策略，对企业和从业者有非常好的借鉴作用，可作为云安全治理，隐私安全评估工作的参考。

报告概述

如何保证云端的医疗健康数据尤其是敏感的隐私数据的安全，需要数据控制者和数据处理者从数据的全生命周期考虑安全，数据安全是数据治理的重要组成部分，在企业数字化转型中需要重点考虑。本白皮书结合业内最佳实践从隐私工程、风险评估、隐私监管几个方面阐述了云端医疗健康数据的保护策略，对企业和从业者有非常好的借鉴作用，可作为云安全治理，隐私安全评估工作的参考。

适宜读者

云安全专业人员、法务、医疗机构网络安全主管、医疗机构IT 主管、IT 审计员和合规人员、第三方风险经理、行业从业者、安全专家、云安全研究、教育、认证、活动者，组织以及云供应商。

扫描公众号二维码，回复“云安全”，获取完整报告

《医疗健康网络安全手册》

报告背景

近年来，网络安全事件频发，事件造成的影响也日益增大，对于医疗健康行业，网络安全的重要性凸显。随着医疗信息化的普及，医疗设备与相关系统的安全性已经关系到医疗机构业务的正常运营。勒索软件，拒绝服务攻击造成的医院应用系统中断，已经给多家医疗机构和患者带来巨大影响。此外，在医疗健康大数据以及医患隐私数据的开发利用过程中，网络安全问题已成为新的行业痛点。网络安全不仅需要在技术层面投入预算提升安全防护水平更需要在网络安全治理管理层面做好设计，在不同业务场景中控制安全风险，提升全员安全意识。本白皮书从全球视角提出了网络安全的发展趋势分析，行业网络安全痛点以及相应的解决方案建议，为企业安全负责人和从业者提供了不错的参考。

报告概述

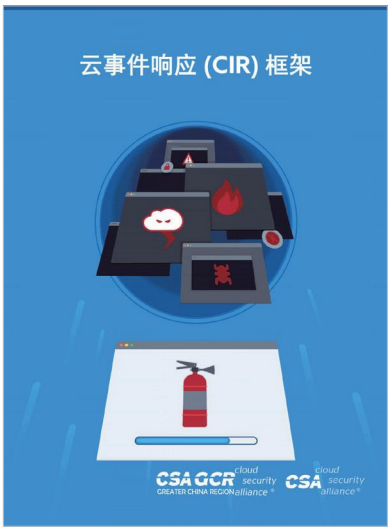
保证医疗健康行业的网络安全，需要企业和个人承担相应的网络安全职责，在中国的《网络安全法》《数据安全法》《个人信息保护法》已经明确要求企业需要委派专人负责，确保网络安全和数据的全生命周期安全。本白皮书从全球视角提出了网络安全的发展趋势分析，行业网络安全痛点以及相应的解决方案建议，为企业安全负责人和从业者提供了不错的参考。

适宜读者

医疗机构网络安全主管、医疗机构IT 主管、IT 审计员和合规人员、第三方风险经理、行业从业者、安全专家。

扫描公众号二维码，回复“云安全”，获取完整报告

《云事件响应（CIR）框架》



报告背景

随着云计算应用的深入，云计算在带来价值的同时，也带来了新的安全与技术挑战。随着《网络安全法》《数据安全法》《个人信息保护法》的相继推出，如何设计有效的纵深实时云安全防御体系成为信息安全从业者亟待解决的首要问题。其中如何制定网络安全事件应急预案、启动应急预案，网络安全信息收集、分析、通报和应急处置等成为困扰很多企业的问题。云计算是一个与传统环境完全不同的领域，将云事件响应与传统事件响应流程区分开来的三个关键方面是治理、可见性和云的责任共享。一个好的事件响应计划有助于确保组织在任何时候都充分准备。

报告概述

本文档旨在提供一个云事件响应（以下简称：CIR）框架，针对破坏性事件的整个生命周期，为CSC提供有效准备和管理云事件的指引。它还可以作为一个透明和通用的框架，为CSP与其CSC共享云事件响应提供最佳实践。CSA旨在为用户提供一个广泛使用的整体框架和一致的视图，目的是为云用户提供有效准备和管理云事件后果的指南，并为云服务提供商与客户共享云事件响应实践提供透明和通用的框架。

适宜读者

云计算管理员、云计算架构师、云计算安全经理、云应用开发人员、云计算软件工程师、基于行业从业者、协会、政府，以及企业和个人会员、安全专家、云安全研究者、教育、认证、活动者，组织以及云供应商。

扫描公众号二维码，回复“云安全”，获取完整报告

《云安全风险、合规性和配置不当报告》

报告背景

云安全联盟（CSA）是一个非营利组织，其使命是广泛推广最佳实践，确保云计算和IT技术中的网络安全。CSA还负责教育这些行业内的各种利益相关者（涉及所有其他形式计算中的安全问题）。CSA的成员是由从业者、公司和专业协会组成的广泛联盟。CSA的主要目标之一是开展调研评估信息安全趋势。这些调研有助于衡量信息安全技术在行业内各方面的成熟度，以及安全最佳实践的采用率。+VMware的CloudHealth®为了增加业界对公有云安全的了解，委托CSA开展一项调查并编写这份调查结果报告。CloudHealth为该项目提供资金，并与CSA一起参与制定针对云安全的调查问题，从而共同制定了该倡议。该调查由CSA于2021年5月至2021年6月在线进行，收到1090份来自不同组织规模和地点的IT和安全专业人士的答复。数据分析由CSA的研究团队进行。

报告概述

云配置不当一直是使用公有云的企业最关心的问题。这种错误会导致数据泄露，允许删除或修改资源，导致服务中断，并对业务运营造成严重破坏。最近，由于配置不当导致的漏洞成为头条新闻，为了更好地了解云安全计划的现状、用于减轻安全风险的工具、企业的云安全态势以及企业在减少安全风险方面面临的障碍，我们进行了这项调研。

知识和专业技能匮乏是信息安全行业内众所周知+的问题。毫不奇怪，知识匮乏和专业技能被一致认定为 通用云安全的主要障碍（59%） 配置不当的主要原因（62%） 主动预防或修复配置不当的障碍（59%）实施自动补救的主要障碍（56%）。

适宜读者

云计算管理员、云计算架构师、云计算安全经理、云应用开发人员、云计算运维人员、安全专家，云安全研究、教育、认证、活动者，组织以及云供应商。

扫描公众号二维码，回复“云安全”，获取完整报告

《企业架构参考指南》

报告背景

纵观一个企业的成长与治理，指南对企业架构建设、优化和运营实践的价值指导意义，在于他抽取、吸收了COBIT、TOGAF、ITIL、SABSA、Jericho、NIST+SP+500-299、+NIST+SP+500-292、ISO27001、ISO+27002等系列框架理论的精要，从而在“云大物智移”环境下，使得企业架构的高效搭建与运行既拥有了理论框架，又有了可查找的实践行动。企业IT治理、安全治理、生产运营、应急事件处理是数字化转型基础内容，指南可服务于对安全、效率和运营有持续优化诉求的大中小企业。

报告概述

本指南展开的对四个域的解构：业务运营支持服务（BOSS)、信息技术运营与支持+(ITOS)+、技术解决方案服务+(TSS)+、安全和风险管理（SRM)。可以用东方人的模式和中国人的，即“你我它”思维思考，你：是指框架中的任何组件、域，我：企业架构的需求、困难、连接方式、紧要度等，它：传递的下一站，实现企业架构期望的目标或阶段方向。

适宜读者

安全架构师、企业架构师、风险管理专业人员、云计算管理员、云应用开发人员、云计算运维人员、安全专家，云安全研究、教育、认证、活动者，组织以及云供应商。

扫描公众号二维码，回复“云安全”，获取完整报告

《云渗透测试指南》

报告背景

在当下日益复杂的网络环境中，评价公有云环境的安全性不能再采用单一的面向云基础设施的安全管控标准，为了充分识别云环境中的安全弱点和系统健壮性，对公有云上运行的系统和服务的渗透测试也成为保障云安全的重要技术手段。

此次发布的《云渗透测试指南》由 CSA 顶级威胁研究工作组专家编写，对当前全球化形势下针对公有云网络空间安全形势、安全风险的实质及特点，提出了应对的渗透测试方法和策略，并且对其中的要点进行了深入分析和阐述。

报告概述

指南基于公有云场景已经达成广泛共识的共享责任模型，从云客户和云服务提供商两个视角对云渗透测试的范围（或边界） 、测试目标、测试用例和关注点、合规性、测试相关培训和资源（如渗透测试工具） 等进行了详尽的阐述。可以指导公有云客户系统全面的逐项评估其云应用、云服务的安全性。指南适用于从决策者到一线渗透测试人员的所有安全从业人员，尤其是云安全从业人员。可以让决策者充分理解云渗透测试的复杂性和重要性，同时为渗透测试人员提供了详尽的用例清单。

适宜读者

安全架构师、渗透测试人员、风险管理专业人员、云计算管理员、云应用开发人员、云计算运维人员、安全专家，云安全研究、教育、认证、活动者，组织以及云供应商。

扫描公众号二维码，回复“云安全”，获取完整报告

《2022中国零信任神兽方阵分析报告》

零信任给广大企业带来了新一代网络安全的战略理念，零信任的落地和价值的发挥是一项复杂工程。作为全球零信任产业引领组织，CSA 为业界更好地促进零信任实施做了大量的贡献，首先将SDP开源贡献给业界形成了由数百家网络安全厂商构成的零信任生态其次推广CZTP零信任专家认证课程，为业界实施零信任培养了上千名网络安全专业人才，而最近建立CSA零信任推进中心，则携手零信任领先厂商们为广大客户们排解落地疑难。此外，云安全联盟大中华区每年举办的国际零信任峰会，已成为全球认可的零信任领域的风向标活动。

2020年开始，云安全联盟大中华区为了向业界完整呈现中国零信任的行业生态，让读者对零信任有一个全面的认知，同时提高零信任领域相关厂商和优秀实践者的曝光度和知名度，为打算实施零信任的甲方提供完整的参考，开始发布《中国零信任全景图》，这项活动已经持续了两年。

云安全联盟大中华区2022年首次推出了《中国零信任神兽方阵报告》，报告采用云安全联盟大中华区原创的中国神兽方阵，该模型是基于中国传统文化创立的分析模型。中国神兽方阵以传统文化的“四象”即青龙、白虎、朱雀、玄武神兽形象为模型，打造具备中国特色的数字安全领域的科技标杆品牌，树立各个细分领域标杆，供市场及用户参考。

《2022 中国零信任神兽方阵》作为零信任首个优秀实践，从技术和市场两个维度评估目前零信任市场的主要厂商，帮助广大厂商和对零信任有兴趣的人员和组织进一步了解该市场的趋势。报告是对《中国零信任全景图》的补充，更关注于对零信任厂商的分析，勾勒出这些厂商在市场上的相对位置，进一步推动零信任市场的健康发展。经过评价筛选，共30家企业入选，其在品牌影响力、技术实力、市场能力、人才潜力方向等综合水平高且各具千秋，是零信任领域科技标杆企业。

扫描公众号二维码，回复“零信任”，获取完整报告

《实战零信任架构》

报告背景

随着组织机构不断将其全部或部分网络迁移到云，政府机构和商业企业的业务负责人必须以新的方式保护其私有、公共或专有云实例。尽管需求迫在眉睫，但安全格局的这种变化的实施需要时间和决心。组织机构将需要通过新技术栈、技能集和流程提高他们在云中保护系统的能力。这对开发新的安全治理和策略提出了挑战，要求基于持续验证、微分段、软件定义网络以及持续监控和持续可见性。为了实施和执行这些现代化策略，行业从业者需要设计和运营传统和现代访问控制和网络技术的复杂组合，并随着时间的推移进行适合自己环境的定制。常见的部署方法（如始终在线的VPN连接和将所有流量路由到企业网关），从成本和用户体验的角度看，变得低效或不再可行。

报告概述

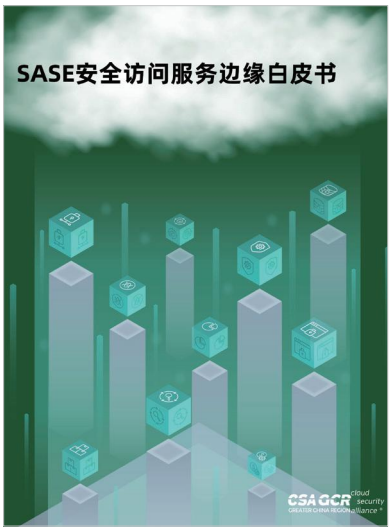
伴随着云原生、DevSecOps在企业内的成功落地，本文在SDP、IAM和微隔离（网络分段）的基础上额外讨论了和容器高度契合的服务网格、边缘计算和策略即代码技术与零信任架构融合的可行性。并从技术、文化、策略及监管措施多个领域分析解决方案影响，帮助行业利益相关方识别挑战和机遇。

适宜读者

IT管理人员、网络安全专家、零信任实施工程师、解决方案专家、企业信息安全管理人员，想要了解如何在组织中实施和管理零信任架构的人员。

扫描公众号二维码，回复“零信任”，获取完整报告

《SASE安全访问边缘白皮书》



报告背景

2019年，Gartner在报告《Hype Cycle for Enterprise Networking 2019》中首次提出了SASE（Secure Access Service Edge）的概念，其核心是网络即服务和安全即服务的融合。Gartner提出这一概念并非空穴来风，而是在当时的国际市场上已有先进服务商在实践网络+安全的融合SaaS服务，并且得到了市场的良好反馈，这意味着随着企业资产云化、办公移动化的深度发展，市场已经产生了对更简洁、统一、融合的SaaS服务的需求。

报告概述

CSA大中华区SASE工作组在《SASE安全访问服务边缘白皮书》中提到，“SASE是企业网络和业务架构演进至“云化”、“服务化”后自然产生的安全架构。”SASE可以在多云、多分支、员工移动办公等场景下为企业提供更好的网络统一性、可见性、安全性，企业使用SASE架构，同步解决广域组网和安全问题，并且安全涵盖全流量、并支持深度威胁检测。这是SASE完整形态的定义，但是由于国内尚在发展早期，工作组也看到目前国内厂商提供SASE服务各有侧重，有基于SD-WAN服务在PoP点增加建设安全服务的，此类服务商在网络服务上则更具经验、优势。有从自身安全服务出发，与网络服务商合作，建设自有SASE服务的，这类SASE服务则更推崇企业以多种方式接入其SASE网络，不强调自身提供SD-WAN服务等，并着重发展的是其安全服务能力优势。

适宜读者

IT管理人员、网络工程师、安全运维人员、网络安全专家，企业管理人员、想要了解如何在组织中实施和管理SASE网络。

扫描公众号二维码，回复“零信任”，获取完整报告

《CISO 研究报告零信任的部署现状及未来展望》

报告背景

零信任作为一种新兴的解决方案，在推广和应用过程中不可避免地会遇到一些问题，零信任的先行实践者们在面对这些问题时也存在一些困惑，这些问题和困惑的存在阻碍了零信任方案的一泛推广。作为零信任的重要推动者，CSA一直专注于零信任方案的研究与创新。CSA在2014年发布了《软件定义边界SDP标准规范1.0》，2022年发布了《软件定义边界SDP标准规范2.0》，并发布了《实战零信任架构》《SASE安全访问边缘白皮书》等一系列规范和报告，为零信任业界提供了重要的参划。为了帮助业界分析零信任研究和实践过程中遇到的问题，CSA组织了本次调研，通过广泛的意见收集和统计，尝试揭示零信任方案落地过程中的障碍。期望通过这些分析，帮助业界找到解决问题的方案。

报告概述

《CISO研究报告：零信任的部署现状及未来展望》本次调研的目的是使大家更好的理解组织机构内部的零信任策略。调研对象要求评估以下方面：

- 零信任在组织机构中的成熟度和优先级
- 采用零信任的好处和驱动因素
- 采用零信任的挑战和障碍
- 支持零信任战略所需的投资

适宜读者

CSO（首席信息安全官）、CIO（首席信息官）、安全分析师、安全工程师、安全顾问、安全架构师等，以及对信息安全领域感兴趣的T从业人员、希望了解“零信任”理

扫描公众号二维码，回复“零信任”，获取完整报告

《基于SDP与DNS融合的零信任安全增强策略模型》

报告背景

国际云安全联盟CSA发布报告《基于SDP和DNS融合的零信任安全增强策略模型》，报告通过2个实际用例解释了如何将DNS、企业管理DDI系统与SDP结合，使用DNS及企业管理DDI系统为SDP提供设备及网络行为的上下文信息，作为SDP系统输入，以增强访问控制策略的决策能力，从而提供改进的安全可见性、恢复能力及响应能力，帮助组织机构通过零信任架构获取的安全保障更上一层楼。

报告概述

域名系统（DNS）是一种分层命名系统，它构建在一个为计算机、服务或任何连接到互联网或专用网络的资源而设的分布式数据库上。动态主机配置协议（DHCP）是一种自动配置协议服务，可在连接时将 IP 地址分配给网络设备，这对于将设备连接到网络至关重要。互联网协议地址管理（IPAM）是企业在私有网络上管理DNS和DHCP的系统。

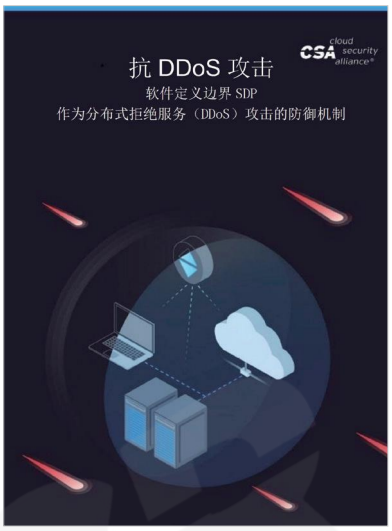
集成上述三个核心网络服务的解决方案统称为 DDI（DNS，DHCP，IPAM）。通过集中式DDI解决方案，网络管理员可以从单一管理平台获得对其网络的可见性和控制权。一个架构设计良好的DDI会使用IPAM集成DNS和DHCP服务的数据，以便每个服务都能及时感知其他服务的变化。

适宜读者

CSO（首席信息安全官）、CIO（首席信息官）、安全分析师、安全工程师、安全顾问、安全架构师等，以及对信息安全领域感兴趣的T从业人员、希望了解"零信任”理念的人士，以及希望了解企业信息安全现状和未来趋势的人士。

扫描公众号二维码，回复“零信任”，获取完整报告

《SDP抗DDOS攻击》



报告背景

SDP 软件定义边界可以有效地防护多种典型 DDoS 攻击手段，包括HTTP Flood,TCPSYN,andUDP Reflection 等。产业界和学术界的一些安全实验室也验证了在拒绝服务攻击实验中，SDP可以允许合法用户机构的访问流量通过，并通知上游路由器区分恶意流量包以迅速对合法网址开绿灯。

CSA 全球（创作）与大中华区（翻译）SDP 工作组的这篇文章为软件定义边界作为防DDoS攻击的新工具打开了天窗，希望读者们通过这篇文章能够认识到SDP 对防御DDoS的作用，并在相关工作中加以应用。

报告概述

分布式拒绝服务（DDoS）攻击是一种大规模攻击。在这种攻击中，攻击者使用多个不同的源IP 地址（通常有数千个）对单一目标进行同时攻击。目的是使（被攻击者的）服务（或网络）过载，使其不能提供正常服务。由于接收到的流量来源于许多不同的被劫持者，使用入口过滤或来源黑名单等简单技术来阻止攻击是不可能的。当（攻击）分散在如此众多的来源点时，区分合法用户流量和攻击流量变得非常困难。一些 DDoS 攻击包括伪造发送方IP 地址（IP地址欺骗），进一步提高了识别和防御攻击的难度 。

适宜读者

本文档的主要目标读者是企业中担任安全、企业架构和法规遵从等角色的人员。这些利害关系人将在很大程度上负责其企业内 DDoS 防御解决方案的评估、设计、部署或运营。其次，解决方案提供商、服务提供商和技术供应商也将从阅读本文档中受益。

扫描公众号二维码，回复“零信任”，获取完整报告

个人信息保护合规准则——中国篇

报告背景

《个人信息保护法》正式实施后，在网信部门的统筹管理下，各行业监管部门也通过开展一系列的行动来推进本行业、本领域开展个人信息保护工作，国家及行业相关配套标准相继发布，但大多数个人信息处理者在个人信息保护合法要求落地实践中仍处于探索阶段，本行为准则在这样的背景下产生。CSA个人信息工作组结合现行法律法规、国家标准及业界最佳实践，为个人信息处理者提供系统性的实施指导，帮助个人信息处理者承担保护用户个人信息的责任，降低合规风险。本行为准则中包含大量来自实际场景的案例或举例，帮助个人信息处理者准确理解控制措施的含义。

报告概述

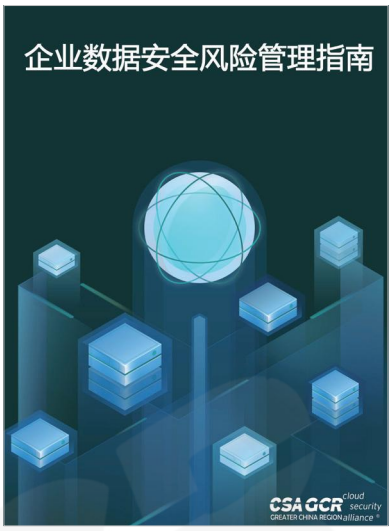
在《个人信息保护法》发布后，大部分个人信息处理者仍在努力识别合规红线，缺乏具有可操作性的实施指导。因此，报告基于《个人信息保护法》制定第一版普适性的行为准则，旨在解决企业的合规挑战，面向所有处于个人信息保护法管辖范围内的个人信息处理者，没有添加行业、领域或规模的限制。

适宜读者

企业或组织的数据保护负责人或数据管理人员、个人数据处理相关的从业人员、关注个人隐私保护和数据安全的个人用户、法律从业人员和相关研究人员。

扫描公众号二维码，回复“数据安全”，获取完整报告

《企业数据安全风险管理指南》



报告背景

数字经济已经成为当今社会快速发展的主流经济，越来越多的国家和企业加速谋划和布局数字经济，抢占发展制高点。我国“十四五”规划中明确提出“加快数字化发展、建设数字中国”的目标，《数字中国建设整体布局规划》发布，在此背景下，我国正处于数字化转型的关键时期，数字技术成为核心引擎，数据成为新的生产要素。云计算、大数据、物联网、人工智能、区块链等新技术正在不断地应用和创新，对数据的开发利用和风险管控已成为当今甚至将来很长一段时间内的热点话题。数据从资源形态通过价值释放转变为资产，通过不断地应用和流通进阶为新的生产要素。数据要素驱动产业数字化转型已经成为全球共识。

报告概述

以合规遵循、业务发展、风险防控等多方面需求驱动，本文构建了以数据为中心的风险管理框架，在充分分析各类数据处理活动场景所面临的数据安全风险的基础上，从数据安全风险管理规划、数据处理活动管理、数据安全风险评估、数据安全风险处置、数据安全风险监督改进、数据安全风险沟通与评审等六大方面给出了切实可行的管理方法，以及通过20套附录工具提供了详尽的实践思路，期望能够为各企业数据安全从业者提供参考和帮助。

适宜读者

关注企业数据安全风险管理的IT从业人员、企业管理人员、信息安全决策者、风险管理专业人员等阅读。本书主要介绍了企业数据安全风险管理的基本概念、方法和实践，以及如何通过数据分类、风险评估和安全控制等手段有效降低企业数据安全风险。阅读本书需要具备一定的风险管理和信息技术基础。

扫描公众号二维码，回复“数据安全”，获取完整报告

《企业网络安全合规框架体系》

报告背景

企业安全需求的驱动力来自合规驱动、事件驱动、风险驱动三部分。安全建设应该考虑云上业务、数据安全、网络安全、个人信息保护、实施零信任架构等方面。需要一份系统性的建设指南参考。例如：云安全合规建设框架涵盖公有云、私有云、混合云和多云场景，从安全管理、安全技术、安全运营和运维几个维度进行设计。数据安全治理体系运行过程包括围绕组织、管理、技术三个维度进行建设，通过定期治理评估发现差距不断完善体系的建设，通过定期审计发现问题，使得数据安全治理体系持续改进。

报告概述

报告方案提出了企业网络安全合规框架体系为“1+2+SEC+N+1”架构。报告包括了云安全合规建设框架、云原生安全合规建设框架、基于等级保护的云安全框架体系、零信任与SASE建设框架、数据安全治理体系、企业个人信息保护体系、数据安全技术体系技术框架及建设分工等大框架，旨在指导更多单位全面开展网络安全合规建设。

企业安全合规视角安全运营框架体系，依托安全技术体系，为安全管理合规提供必要的支撑与输入，在当前多样安全标准、安全监管的态势下，形成符合企业自身的合规图谱，实现安全合规可量化、可展示，提升合规响应效率，降低安全合规风险。

适宜读者

关注企业网络安全合规的IT从业人员、企业管理人员、信息安全决策者、网络安全顾问和安全评估人员等阅读。本方案主要介绍了企业网络安全合规的相关法律法规、标准和规范，以及企业应如何建立符合安全合规要求的网络安全框架体系。阅读本方案需要具备一定的网络安全和信息技术基础。

扫描公众号二维码，回复“数据安全”，获取完整报告

《云上数据安全与重要事项》

报告背景

BigID委托CSA进行了一项调查和报告，以便更好地了解业界对云数据安全的认知、态度和意见。BigID资助该项目并联合CSA研究分析师共同制定了调查问卷。CSA于2022年7月通过线上开展这项调查，收到了1633份回复，分别来自不同规模、不同地点组织内的信息技术和安全专业人员。CSA的研究分析师对这份报告进行了数据分析和说明。

报告概述

通过线上开展这项调查，收到了1633份回复，分别来自不同规模、不同地点组织内的信息技术和安全专业人员。CSA的研究分析师对这份报告进行了数据分析和说明，阐述了4个重要发现，重要发现1：各组织正在努力保护和跟踪云中的敏感数据；重要发现2：第三方和供应商对敏感数据的访问权限相似；重要发现3：暗数据问题源于人员配置问题和部门间的冲突；重要发现4：大多数安全专业人士认为，他们的企业明年将会遭遇数据泄露。此调查报告总结详尽，数据分析维度值得参考。

适宜读者

云计算安全和数据安全的IT从业人员、网络安全爱好者、企业管理人员、信息安全决策者等阅读。阅读本书前需要具备一定的计算机和网络安全知识基础。

扫描公众号二维码，回复“数据安全”，获取完整报告

《物联网安全关键技术白皮书》

报告背景

未来的世界是一个万物智联的世界，人们的工作生活将无时无刻被各种物联网设备紧密地绑定到一起。可以预见物联网的安全将是未来现实世界的重要组成部分，不仅关乎信息和隐私，更会关乎人民生命财产。

报告概述

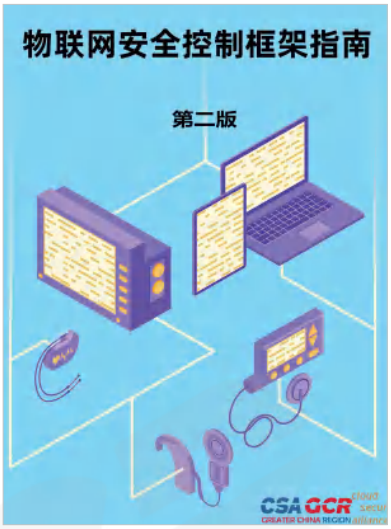
在本次发布的白皮书中，CSA大中华区物联网安全工作组从分析物联网的架构、威胁出发，重点对各种物联网安全技术进行深入剖析，从底层芯片到上层APP测试，通盖物联网安全的各个方面，希望能够帮助读者快速的掌握在物联网安全中可以用到的各种关键技术，这些技术可以应用到物联网产品或解决方案中，为提升产品或解决方案安全性、保护用户隐私、提升用户体验起到有效作用。本白皮书还对这些关键技术的应用场景做了分析和建议，以帮助读者在实际场景中选择合适的物联网安全技术，更好地发挥技术的能力，创造一个更加安全的物联网环境。

适宜读者

从事物联网相关工作、企业管理、信息安全相关工作或物联网技术研究的人员。

扫描公众号二维码，回复“物联网”，获取完整报告

《物联网安全控制框架指南》（第二版）



报告背景

随着5G的大规模商用，以及云计算、AI等不断的成熟和应用，万物物联成为全球网络未来发展的重要方向，在工业领域、智慧城市、车联网、智能家居、智慧穿戴等领域发挥重要作用。在一片物联网蓬勃发展的局面下，我们也不能忽视，物联网安全是物联网能够广泛应用的先决条件。随着越来越多的物联网终端接入到网络中，大量的数据接入点被添加到物联网系统中，这为企业的整体物联网安全防护提出严峻的挑战。因此CSA云安全联盟推出了物联网安全关键技术白皮书，旨在帮助广大的企业面对物联网的安全挑战时能够有所参考和依据，本白皮书的内容对于如何做好物联网的安全防护、安全检测有现实的参考作用。在使用中可以根据自己的实际情况进行适配。

报告概述

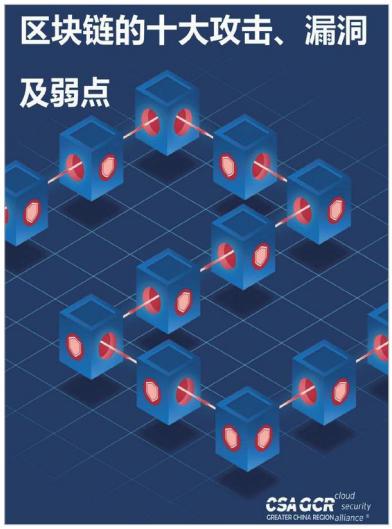
云安全联盟（CSA）物联网安全控制框架为希望更好地理解和实施其物联网体系结构中安全控制项的组织提供了一个起点。框架随附的本指南解释了企业组织如何使用该框架安全地评估和实施物联网系统。物联网安全控制框架用于部署各种互联设备和相关云服务、网络技术和应用软件的企业物联网系统。该框架在许多物联网领域都具有效用，从只处理影响力有限的“低价值”数据系统到支持关键服务的高敏感系统。系统所有者根据存储和处理的数据价值以及各种潜在的物理安全威胁影响对组件进行分类。

适宜读者

物联网安全控制框架是系统架构师、开发人员和安全工程师的一个资源，用来设计安全的物联网生态系统。物联网系统评估人员（如审计师和渗透测试人员）可以利用该框架来验证控制及其部署的实施情况。

扫描公众号二维码，回复“物联网”，获取完整报告

《区块链的十大攻击、漏洞及弱点》



报告背景

分布式账本技术（LT）被称为技术基础结构和协议，用于在分布于多个位置的网络中以不变的方式进行验证，同时访问和记录更新。由于DLT在各个领域和行业中的潜力，因此在技术领域正变得越来越流行。自12年前比特币问世以来，加密货币和支持它们的平台一直是攻击的目标。攻击者期望的结果是尽可能多地偷取加密货币利润。为实现这一目标，不良行为者可以针对区块链协议本身攻击特定平台。

报告概述

《区块链的十大攻击、漏洞及弱点》这份报告覆盖了针对加密货币和LT的十大攻击类型。也对这十大攻击类型进行了整体概述。虽然每种攻击类型都可以成为一篇单独的文章，因为篇幅有限，在此次报告中只总结描述了十大攻击，并提供了说明性示例和代价高昂的教训。

适宜读者

本文可以帮助开发者，安全合规人员以及日常加密货币用户教育自己如何避免落入许多相同的陷阱。文章深入浅出，总结详尽，值得大家参考。

扫描公众号二维码，回复“区块链”，获取完整报告

《区块链数据层安全与隐私保护设计指南》

报告背景

随着新兴技术如区块链、人工智能等飞速发展，区块链逐新成为“价值互联网”的重要基础设施，各国都开始积极拥抱区块链技术，开辟国际产业竞争的新赛道。区块链自身有着分布式、点对点传输、透明、可追踪、不可篡改、数据安全等特点，在某种程度上解决了数据的完整性、真实性及唯一性等问题，使得用区块链技术解决数据安全与隐私的问题成为人们竞相关注的焦点。

报告概述

本文档从区块链数据概念与范畴、数据格式入手，分析区块链数据安全与隐私保护的需求，从接入层、处理层及展示层的设计指南全面呈现数据安全与隐私保护总体框架，并提供测试指南，最后以区块链数据安全应用场景收尾。文章内容深入浅出，是研究区块链数据安全与隐私保护领域很好的参考材料。

适宜读者

区块链开发者、技术架构师、安全专家，区块链应用开发，区块链技术研究的人员，数据安全和隐私保护工作的人员区块链相关工作、区块链应用开发、区块链技术研究、数据安全和隐私保护等领域的人员，或者对区块链数据层的安全和隐私保护设计感兴趣。

扫描公众号二维码，回复“区块链”，获取完整报告

《共识算法与共识安全》

报告背景

从早期的分布式一致性算法的缓慢发展到现如今区块链共识的百花齐放，共识算法的发展已经走过了四十年左右的时光。随着区块链技术的快速发展，共识算法也在不断演进和提高，不同的共识算法的侧重点不同，因此它们所面临的问题、环境也不一样。共识算法，可以理解为是为了实现分布式一致性协议而产生的一系列流程与规则。当分布在不同地域的节点都按照这套规则进行协商交互之后，最终总能就某个问题得到一致的决策，从而实现分布式系统中不同节点的一致性。

报告概述

《共识算法与共识安全》白皮书深入介绍了CFT类共识算法、经典拜占庭共识和开放BT类共识等三大类共识算法，并延伸到了共识算法安全性分析和测试方法。报告旨在提供一份系统的关于共识算法安全的知识，从共识算法理论和实现两方面展开安全测试和分析，理论分析主要从算法本身展开分析，实现分析从算法的具体参数、代码实现、应用部署等都方面进行安全分析和测试。基于测试方法和标准，对共识算法安全的典型安全进行分析，并给出分析过程和结论。报告以超级账本和以太坊共识算法为例，探索这些项目在共识算法安全领域的实践经验。报告旨在为区块链开发者、投资者、组织机构在共识算法安全领域提供指导，通过详细数据和案例进行论证，力求将理论与实践更好结合，希望能为您提供有关共识算法的有益信息，帮助您更好地理解和应用这项技术。

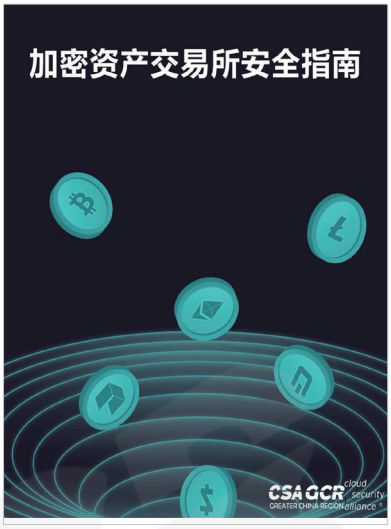
适宜读者

区块链从业人员，区块链研究人员，区块链爱好者，从事密码学、分布式系统、网络安全等领域研究的学术研究者。

扫描公众号二维码，回复“区块链”，获取完整报告

《加密资产交易所安全指南》

报告背景



区块链作为一种颠覆性技术，能帮助多个应用场景的业务创新并促进业务转型。区块链的去中心化和不可篡改的特性可以使交易双方安全可信地执行交易、验证交易和审计历史交易。在政务、金融、身份管理、医疗健康、智能家居和物联网、供应链和物流、汽车行业等多个细分领域中有很多新兴应用案例。同时，区块链技术也面临着诸多的安全挑战，与传统信息系统的安全架构相比，与加密资产交易所相关的系统架构、运作的边界、参与者和组件已重新定义，给用户，区块链服务提供机构及监管机构带来了全新的安全及监管的挑战。

报告概述

本指南对于加密资产交易相关的安全威胁、安全架构、最佳安全实践、应对相关威胁的控制措施提供了指导，可以很好地帮助加密资产交易用户、服务提供机构及监管机构提升安全意识，了解相关威胁及防护措施。文章结构清晰，内容简洁，值得参阅。

适宜读者

加密资产交易所从业人员，加密资产投资者，区块链技术爱好者，区块链研究人员《加密资产交易所安全指南》适宜所有对加密资产交易所的安全性能感兴趣或需要了解加密资产交易所的安全性能的人士阅读和学习。

扫描公众号二维码，回复“区块链”，获取完整报告

《Hyperledger Fabric2.0 架构安全报告》

报告背景

《Hyperledger Fabric2.0架构安全报告》是由Hyperledger社区发布的一份关于Hyperledger Fabrica2.O架构安全性能的报告。Hyperledger是一个由Linux基金会主持的开源区块链项目，致力于推动区块链技术在企业领域的应用。Hyperledger Fabric是HyperledgerI项目的一种实现，是一种可扩展的企业级区块链解决方案。

报告概述

作为一种重要的区块链解决方案，Hyperledger Fabric的安全性能一直是人们关注的焦点。为了进一步了解Hyperledger Fabrica2.O的安全性能和架构特点，Hyperledger社区发布了这份《Hyperledger Fabric2.0架构安全报告》，对Hyperledger Fabrica2.O的安全性能和架构进行了深入的分析和评估，并提供了有价值的安全建议和指导。

该报告主要介绍了Hyperledger Fabric2.O的安全架构和设计特点，分析了Hyperledger Fābic2.0在身份验证、授权和机密保护等方面的安全性能，并提供了一些安全建议和指导，以帮助企业更好地保障其Hyperledger Fabric2.O应用的安全性能。

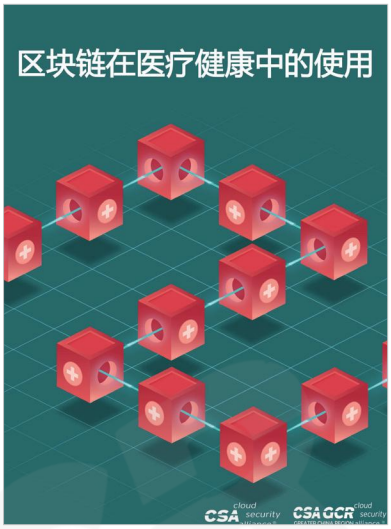
适宜读者

区块链从业人员，区块链技术爱好者，企业安全从业人员，区块链安全研究人员。

扫描公众号二维码，回复“区块链”，获取完整报告

《区块链在医疗健康中的使用》

报告背景



医疗健康数据的独特属性使其成为不法行为者的主要目标。可以预见的是，医疗健康信息受到美国和欧盟隐私及安全法律、管理云数据存储的国际规则的严格监管。数据的高价值再加上这些监管要求，促使各类组织探索使用区块链保护数据。区块链是一个由“一组区块”组成的数字账本。添加到新块中的事务在验证后才加到块中。区块完成时，将按时间顺序追加到现有区块链的末尾。区块链是唯一的，因为只有两个可能的事务：“添加事务”和“查看事务”。事务永远不能被删除或编辑。这一有限的行动集有助于确保数据完整性——这是医疗健康的关键元素，也是不可否认性。区块链可以实现高效的医疗健康数据共享，同时确保患者隐私和数据安全。

报告概述

本文中对区块链在医疗健康行业中的应用进行了背景、技术、案例、展望等全方面多层次的介绍与分析，对于把握行业前沿以及发展情况有重要的指导意义。

提供医疗信息服务提供商如何向其客户提供安全的云解决方案（服务、传输、应用程序和存储），并在医疗健康和相关行业的所有方面促进云意识。随着医疗设备和连接到云的物联网连接数增加，安全性和隐私已成为医疗健康提供组织的重要关注点。将帮助定义医疗健康提供组织在云中安全运行的流程。此外，鼓励医疗健康提供组织、云服务提供商和设备制造商在协作环境中工作，以确保患者的安全以及医疗健康数据的安全和隐私。

适宜读者

医疗从业人员，区块链从业人员，医疗健康管理者和决策者，区块链和医疗健康领域的研究人。

扫描公众号二维码，回复“区块链”，获取完整报告

《隐私科技白皮书》

报告背景

在隐私科技蓬勃发展的短暂历程中，各家对隐私科技都有着不同的定位，是硬核技术？是数据合规的基础架构？是监管科技？是法律科技？抑或是合规科技？这表明了隐私科技覆盖了很大的范畴。隐私科技不同的定位将催生出诸多细分的赛道和领域，并且不同的细分赛道和领域之间将相互作用和协同，最终形成隐私保护合规的新生态链。在撰写本白皮书的期间，围绕着隐私计算，隐私科技涌现出大量的研究与调研的报告和白皮书，我们正处在一个隐私科技急速发展的时期。可以预见在未来的几年内，市场上将涌现出大量的隐私科技新技术，新赛道和新厂商。随着隐私合规落地实施与运行的不断深入，隐私科技市场的趋势也会随之不断变化，并在这一过程中不断迭代，演进，持续赋能隐私合规。

报告概述

这本白皮书由CS隐私科技工作组编写，CSA大中华区专家组评审。近年来，国家层面相继发布了多部个人信息保护与网络安全、数据安全相关的法律法规，保障国家安全、公共利益和个人隐私权益。如何在满足法律合规要求、保障个人安全性、保护个人隐私权益的同时，促进个人信息的有序流动与使用。本书从隐私合规、数据安全、数据可用的维度出发，开创性地提出了“隐私科技”的概念，详细描述了其定义、发展历程、技术以及应用场景，分析了全球以及中国的隐私科技产业环境，同时深入浅出地描绘了隐私科技的发展趋势，值得大家参考。

适宜读者

数据保护从业人员、科技从业人员、法务人员、学生和研究人员、适宜所有对隐私保护感兴趣或者需要了解隐私保护相关技术和方法的人士阅读和学习。

扫描公众号二维码，回复“隐私保护”，获取完整报告

基于《个人信息保护法》的企业个人信息保护合规风险控制验证框架 1.0

报告背景

《个人信息保护法》《网络安全法》施行后，相关行业、企业已经开发了一些合规工具，有些是基于既有安全产品，如典型的安全厂商的合规技术产品，也有是在安全咨询、服务方法论和风险管理理论基础上进行的升级，如ISO标准、数据安全成熟度模型，还有从法律法规出发进行的设计，比如工信部、汽车行业的数据安全指引文件，以及直接以监管机构的检查活动，比如APP收集使用个人信息清单进行逐项符合的因应等等。

报告概述

目前个人信息保护的主要原则可以概括是为：合法正当必要性原则、合理直接目的性原则、最小影响和最小范围原则。将这些确定为原则，主要原因是对必要性、合理性、最小化这些概念难以和缺少准确的衡量指标，且新技术、新应用又不断地冲击既有的量化标准。由于这些原则具有在产品、服务设计中的普遍适用性，且在进行是否合规的“终极”判定时，或者在无其他明确法律依据支持佐证时，需要直接援引这些原则判断。因此，就其中最为基础的必要性原则，也称之为个人信息保护合规判定的“帝王原则”。值得注意的是，这些原则判断的最终权，在监管机构（执法）和司法机关。合规工作虽然可以减轻或降低风险后果，但不能完全免责。框架主要从法律规定出发，而非从单一的权利主体个人视角或者从监管角度、技术角度，尝试建立一个可自洽并周延的体系。为此主要使用了以下方法和逻辑。

适宜读者

企业信息安全管理人员、企业高层管理人员、信息安全从业人员、任何对企业个人信息保护合规有兴趣或需要了解的人士，都可以阅读该框架进行学习和了解。

扫描公众号二维码，回复“隐私保护”，获取完整报告

《基于NIST网络安全框架的勒索软件风险管理内部报告》

报告背景

2022 年 2 月，美国商务部下设的国家标准与技术研究所 (NIST) 发布了最终版《基于 NIST 网络安全框架的勒索软件风险管理内部报告》，这是对 2020 年以来重大勒索攻击事件从技术和管理层面的整体策略回应，同时也是履行其基于 2014年《网络安全促进法》和制定、完善《提升关键基础设施网络安全框架》的行政职责。

报告概述

CSA 大中华区隐私与个人信息保护法律工作组翻译了该文件（有删减），以及对国内的关键信息基础设施保障和提高应对勒索攻击的能力上有所借鉴，特别是在支持《关键信息基础设施安全保护条例》制度落地的方法论和策略方面，且在具体的应用场景上与网络安全等级保护的措施形成有益的补充和对照。

值得注意的是，本报告的风险控制主要是在组织层面实现，这与《关键信息基础设施安全保护条例》专章突出行业、领域的保护工作部门的机制有所不同，企业在参考时应予以关注和区别。

适宜读者

本报告的适用对象是拥有可能遭受勒索软件攻击的网络资源的任何组织，无论所在行业或规模如何。任何组织：中小型企业（SMB)、小型联邦机构和其他小型组织，以及工业控制系统（CS）或运营技术（OT）的运营商都可以利用本报告。

扫描公众号二维码，回复“隐私保护”，获取完整报告

CSA办公室微信

公众号

国际云安全联盟大中华区

电话: 0755-86548359

官网: https://c-csa.cn

邮箱: info@c-csa.cn