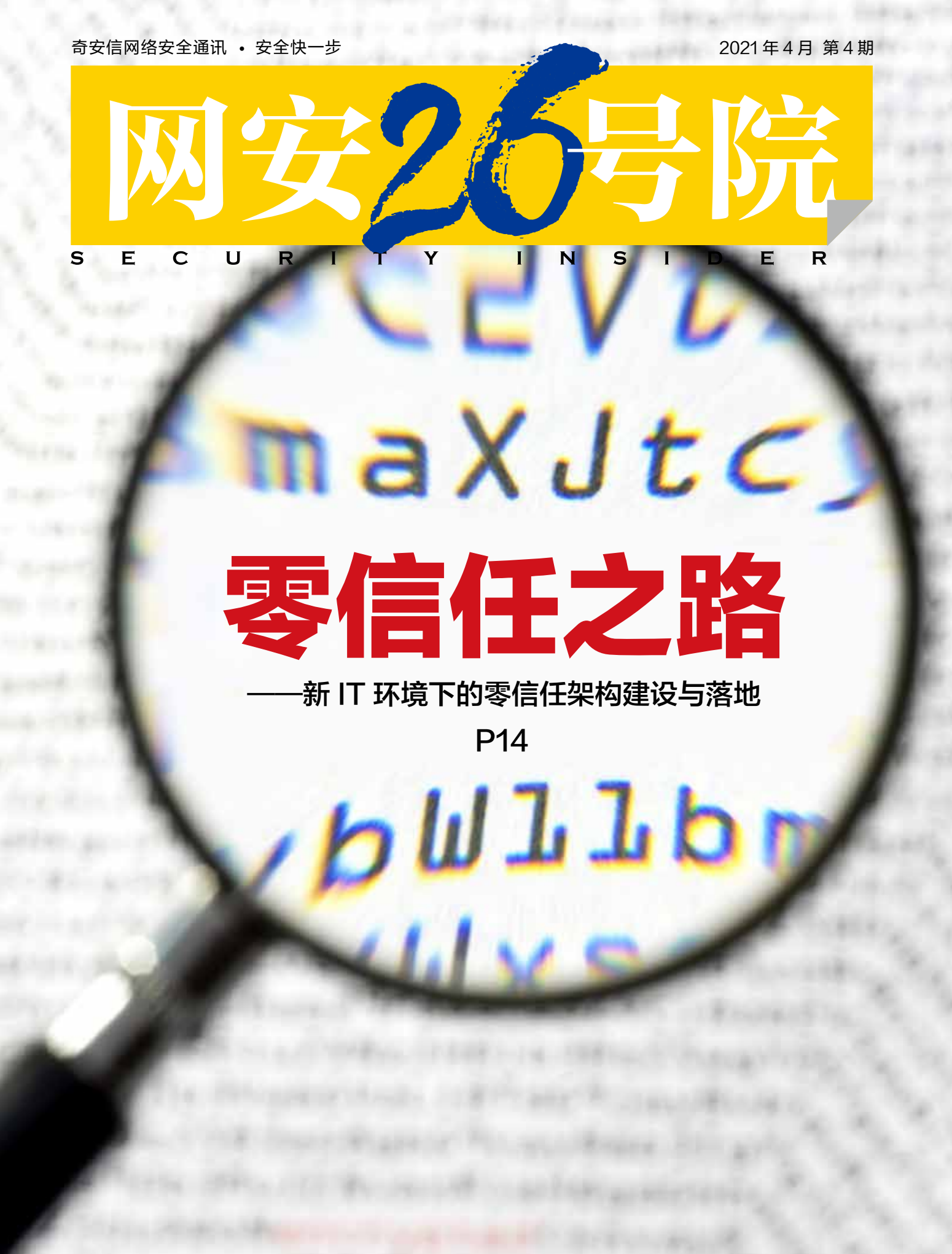
奇安信网络安全通讯 • 安全快一步

2021 年 4 月 第 4 期

网安26号院

SECURITY INSIDER



零信任之路

——新 IT 环境下的零信任架构建设与落地

P14

规划快一步

奇安信 | BEIJING 2022

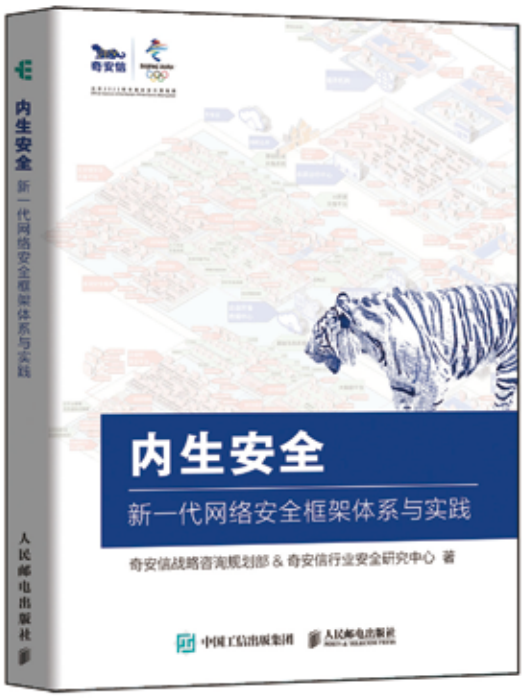
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

新书发布

内生安全权威解读

19支团队、37位专家倾力打造

政企“十四五”网络安全规划必读书籍



- 什么是内生安全
- 内生安全从何而来
- 为什么要内生安全
- 内生安全如何落地
- 新一代网络安全框架
- “十工五任”建设要点

扫描二维码
专享内购价

2021: 零信任安全年?

过去一年多的疫情令远程办公成为风潮，加速了机构的数字化转型，多云和混合网络环境成为企业的常态，攻击面呈指数级增长，基于边界的传统安全防护手段日渐式微；攻击者却变得越来越聪明，手段越来越高级，资源也越来越多，惊人的数据泄露事件频发。

在美国，最近数月发生的安全事件暴露出防护中的缺陷，政府官员和安全从业者视零信任为应对混乱的救命稻草。2021 年 2 月，美国国家安全局（NSA）发布零信任指南，敦促与国家安全和关键基础设施相关的网络所有者，采用零信任安全模型。3 月，美国首席信息安全官 Christopher DeRusha 在听证会上表示，正与美国政府机构合作以实现零信任。美国国防部首席信息安全官戴维 · 麦基翁则表示，国防部正筹建专门协调实施零信任安全架构的投资组合管理办公室。

至此，零信任安全模型被行业领袖所接受，2021 年甚至被称为零信任安全年。而 10 年前，研究员约翰 · 金德瓦提出“不应信任网络中的任何人”时，却被人们认为是句“疯话”。

在国内，“零信任”也已经成为安全领域最热门的词汇。头部客户已经广为接受零信任概念，也出现了专做零信任产品的创业公司；过去从事 IAM、VPN、微隔离的厂商纷纷打上零信任的标签。各大安全厂商也纷纷推出零信任解决方案。根据 MarketsandMarkets 的数据，全球零信任安全市场规模预计将从 2020 年的 196 亿美元增长到 2026 年的 516 亿美元。

尽管各方看好，零信任之路却没有捷径，无疑是一场漫长的旅程。有专家认为，大型机构预计将需要近十年的时间才能真正实现全面的零信任安全。国家安全局（NSA）在指南中，不建议现在就实施全面的零信任，并将零信任过渡分为四个关键阶段：准备阶段，基本阶段，中间阶段和高级阶段。2016 年的一份美国国会报告，要求政府网络采用零信任模型。但在 5 年后的今天，零信任仍然还只是大部分美国政府机构的一项雄心勃勃的目标。

在本期的零信任专题中，除了介绍最新的零信任进展以及适用场景，还重点介绍了几个典型案例，希望可以成为确定零信任安全建设方向与重点的参考。

总编辑

李建平

2021 年 4 月 1 日

CONTEN

目录

TS

安全之道

奇安信人

奇安资讯

第 4 期

《网安 26 号院》编辑部

主办 奇安信集团

总　　编　　辑：李建平
副　　总　　编：裴智勇
安全态势主编：王　彪
月度专题主编：李建平
攻防一线主编：魏开元
安全之道主编：张少波
奇安信人主编：孙丽芳
奇安资讯主编：陈　冲
安全意识主编：李建平

奇安信集团　虎符智库　安全内参

电子版请访问 www.qianxin.com 阅读或下载
索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

Email: 26hao@qianxin.com
地 址：北京市西城区西直门外南路 26 院 1 号
邮 编：100044
电 话：（010）13701388557
出版物准印证号：京内资准字 2021- L0058 号
印刷数量：45000 本
印刷单位：北京七彩虹印刷有限公司

事件篇

美国又双叒遭遇重大供应链攻击，热门开发工具 Codecov 遭篡改导致数万家机构的开发环境凭证信息暴露，可能引发大规模泄密事件，FBI 正在紧急调查事件影响；伊朗核设施建成后一天便遭遇重大故障下线，外界纷纷传言是以色列特工发动网络攻击，但伊以双方却不予置评，此间疑云重重；宏碁电脑遭勒索攻击被开出天价赎金，高达 3.25 亿人民币……

热门开发工具 Codecov 遭篡改，全球数万机构敏感信息或暴露

据 Bleeping Computer 4 月 16 日消息，国际代码测试领导厂商 Codecov 发布公告称，旗下代码测试软件遭到黑客篡改，客户持续集成（CI）环境中的凭据信息遭暴露，可借此访问服务器窃取敏感数据。该软件在全球范围内有 2.9 万名客户使用，包括宝洁、GoDaddy、华盛顿邮报、加拿大皇家银行等，可能爆发大规模数据泄密事件，FBI 已经紧急启动影响评估调查。Codecov 在 4 月 1 日获悉此事，立即采取了修复措施。不过调查认为，这起软件供应链攻击早在今年 1 月末就已发生，攻击者潜伏了长达 2 个月之久。有专家认为，其影响范围或将比拟数月前的 SolarWinds 供应链投毒事件。

震网攻击重现？疑似以色列网络攻击伊朗核设施导致断电

据 The Register 4 月 12 日消息，伊朗官方称，纳坦兹核设施在周末发生故障，被迫断电下线。该设施在前一天正式建成，被认为具备浓缩铀的能力，突破了美伊核协议谈判的限制。伊朗官员表示，对纳坦兹核设施的打击是一次核恐怖主义行为。消息公布不久后，多家以色列媒体报道称，这其实是以色列情报机构摩萨德策划的一次网络攻击。以色列官方不予置评。

华为应用商店被曝 10 款恶意软件，已有超 50 万用户下载

据 The Record 4 月 9 日消息，俄罗斯安全公司 Dr. Web 发现，华为应用商店 AppGallery 中 3 个开发人员的 10 款应用程序感染了恶意软件 Joker，会进行 WAP 欺诈，为用户偷偷订阅付费电信服务。这 10 款应用包括虚拟键盘、相机、应用启动器、通讯工具等。华为收到提醒后，在应用商店删除了这些应用。据统计，这些应用有超过 50 万次下载。近几年来，谷歌 Play 商店已经检测并删除 1700 多个包含 Joker 恶意软件的应用。

Facebook 超 5.33 亿用户的账号和电话信息泄露

据 The Hacker News 4 月 4 日消息，地下论坛曝光，有人放出了 5.33 亿 Facebook 用户的信息，任何人均可免费下载。泄露信息包括用户名、手机号、位置、

邮箱等，涉及 106 个国家 / 地区。据分析，这些数据似乎是利用 Facebook 的一个接口漏洞抓取。有研究员发现，泄露数据里还有 Facebook 创始人兼 CEO 扎克伯格的账号和手机号。Facebook 官方回应称，泄露数据为 2019 年报告的老数据，漏洞已于 2019 年 8 月修复。

供应商遭恶意软件攻击，美国八个州汽车无法年检

据 Bleeping Computer 4 月 3 日消息，美国排放测试公司 Applus Technologies 3 月 30 日遭到恶意软件攻击，IT 系统被迫断开连接，旗下车辆排放测试平台也无法访问，致使八个州的汽车无法年检。Applus Technologies 目前无法提供恢复服务的时间表，受影响州的汽车管理机构表示，年检可能要到 4 月 6 日甚至更久才能恢复。

30 个 Docker 镜像存在恶意挖矿代码，总下载数超 2000 万次

据 Security Affairs 3 月 30 日消息，美国安全公司 Palo Alto Network 的研究员发现，全球最大的镜像社区 Docker Hub 镜像社区里有 30 个镜像存在恶意挖矿代码，这些镜像被下载超过 2000 万次。据统计，这些镜像共产生了价值 20 万美元的加密货币，其中 90% 以上是 Monero 加密货币，其次是 Grin、ARO。

澳大利亚第九频道遭勒索攻击，电视直播被迫中断超 24 小时

据 Security Affairs 3 月 28 日消息，澳大利亚第九频道遭网络攻击，导致周日上午的电视直播无法进行，新闻节目被迫中断。该公司内部邮件称，系统遭到史无前例的网络攻击，IT 网络受到严重影响，但邮件系统正常。到下午 6 点，新闻节目才正常播放。后续，该公司表示，是遭到了大规模勒索软件攻击，整个内部网络瘫痪，有消息人士称，这可能是俄罗斯的报复攻击，以阻止该节目周一的普京总统调查新闻。

选举前一天，以色列 650 万选民信息全部曝光

据 Security Affairs 3 月 24 日消息，在以色列新一轮大选的数小时前，数百万公民的个人身份与选举登记信息遭到大规模外泄，泄露数据包括登记选民的住址、电话号码和出生日期等。据报道，攻击者在前一周入侵了选举应用 Elector 背后的开发运营公司 Elector 软件，并窃取到大量数据。Elector 公司已经收到威胁消息，要求立即停止运行 Elector 应用，被拒绝后公布了数据。目前，包括执政党利库德党在内的多个党派都在使用这款软件。

宏碁电脑遭勒索攻击：赎金 3.25 亿元创下最高纪录

据 BleepingComputer 3 月 19 日消息，电脑巨头宏碁（Acer）遭遇 REvil 勒索软件攻击，攻击者开出了迄今为止最高数额的赎金 5000 万美元（约 3.25 亿人民币）。REvil 勒索软件团伙在其数据泄露网站上声称已成功入侵宏碁的系统，并公布了数张被盗文件截图，包括财务表格、银行往来信息等。宏碁官方未回应此事，仅强调已向相关部门上报了近期发现的异常情况。

漏洞篇

4月的空气弥漫着硝烟战火。实战攻防演习期间，国内互联网上到处流传着各种版本的漏洞利用代码。从OA、邮箱、运维、安全产品到浏览器、聊天工具，以往我们认为安全可信赖的系统，纷纷开启紧急更新模式。安全管理员已启动全体循环广播：请升级软件！

开源搜索服务 Apache Solr 多个高危漏洞预警

2021年4月19日，网络安全威胁和漏洞信息共享平台监测到Apache官方发布Apache Solr安全更新公告，修复了Apache Solr存在的服务器端请求伪造漏洞、敏感信息漏洞以及数据集读写漏洞，对应CVE漏洞编号：CVE-2021-27905，CVE-2021-27262，CVE-2021-27905。其中Apache Solr服务器端请求伪造漏洞（CVE-2021-27905）的PoC已在互联网公开，漏洞影响较大。建议受影响用户将Solr升级至8.8.2或更高版本进行防护，做好资产自查以及预防工作，以免遭受黑客攻击。Apache Solr是美国Apache软件基金会的一款基于Lucene（全文搜索引擎）的搜索服务器。

谷歌 V8 引擎远程代码执行漏洞导致微信等软件存在关联漏洞的安全通告

2021年4月17日，国家信息安全漏洞共享平台收录了微信Windows客户端远程代码执行漏洞（CNVD-2021-29068），此漏洞是Google V8引擎历史漏洞（CNVD-2021-29059，对应CVE-2021-21220）的衍生关联漏洞。微信Windows客户端使用V8引擎解析JavaScript代码，并关闭了沙盒模式。攻击者利用该漏洞，通过发送钓鱼链接并引诱用户点击，可获取远程主机控制权限。目前，漏洞细节已公开，厂商已发布新

版本完成修复。

谷歌公司开发维护的V8引擎是一款开源JavaScript引擎，其不仅被广泛应用于Chrome、Edge等浏览器软件中，而且在内置网页浏览功能的软硬件产品中得到了广泛应用，例如微信。近几年，V8引擎曾多次被研究者发现存在高危漏洞。其中，Google V8引擎远程代码执行漏洞（CVE-2021-21220）相关细节已公开，谷歌公司尚未发布新版本修复该漏洞。未经身份验证的攻击者利用该漏洞，可通过精心构造恶意页面，诱导受害者访问，实现对浏览器的远程代码执行或者拒绝服务攻击，但攻击者单独利用上述漏洞无法实现沙盒（SandBox）逃逸。

微软 Exchange 服务多个远程命令执行漏洞预警

2021年4月14日，网络安全威胁和漏洞信息共享平台监测到微软发布Exchange安全更新通告，修复

了 4 个远程命令执行漏洞（CVE-2021-28480,CVE-2021-28481,CVE-2021-28482,CVE-2021-28483）。攻击者利用漏洞可绕过 Exchange 身份验证，从而实现远程命令执行。同时，这些漏洞是蠕虫级的，可在内网的 Exchange 服务器间横向扩散。建议受影响用户及时更新漏洞补丁进行防护，做好资产自查以及预防工作，以免遭受黑客攻击。据悉，这 4 个漏洞是美国国家安全局报告给微软。

谷歌 Chrome 浏览器多个远程命令执行漏洞安全通告

2021 年 4 月 13-14 日，奇安信 CERT 连续监测到互联网上公开谷歌 Chrome 浏览器多个远程命令执行 0day 漏洞的利用代码（PoC）。4 月 13 日，有研究员披露了一枚 Chrome 远程命令执行 0day 漏洞（暂无编号）的 PoC，影响当时的 Chrome 浏览器最新版（v89.0.4389.114）；4 月 14 日，互联网上又公开一枚谷歌 V8 引擎的远程命令执行 0day 漏洞（CVE-2021-21220）的 PoC，影响当时的 Chrome 浏览器最新版（v90.0.4430.72）和 Edge 浏览器最新版（v89.0.774.76）。攻击者构造特殊的 web 页面诱导受害者访问，均可实现远程代码执行。

致远 OA 旧版本用户存在安全隐患应及时进行修复的风险提示

2021 年 4 月 10 日，国家信息安全漏洞共享平台发现致远 OA 旧版本的用户由于未及时更新厂商补丁，存在安全隐患。由于致远 OA 软件旧版本（V8.0 以下，V8.0 于 2020 年 6 月 11 日发布）集成的 Fastjson 组件存在反序列化漏洞，攻击者利用该漏洞，可在未授权的情况下获取目标服务器权限，实现服务器的远程代码执行。目前，漏洞利用细节已小范围公开，厂商已于 2020 年 9 月发布补丁完成修复。

亿邮电子邮件系统远程命令执行漏洞安全公告

2021 年 4 月 10 日，国家信息安全漏洞共享平台收录了亿邮电子邮件系统远程命令执行漏洞（CNVD-2021-26422）。攻击者利用该漏洞，可在未授权的情况实现远程命令执行，获取目标服务器权限。目前，漏洞利用细节已公开，厂商已于 4 月 9 日发布版本补丁完成修复。亿邮电子邮件系统是由北京亿中邮信息技术有限公司开发的一款面向中大型集团企业、政府、高校用户的国产邮件系统。

奇安信 CERT：近期需重点关注的 26 个高风险漏洞

2021 年 3 月，奇安信 CERT 监测到新增漏洞 2275 个，其中有 852 条敏感信息触发了人工研判标准。经人工研判，本月值得重点关注的漏洞共 141 个，其中高风险漏洞共 26 个，包括多个遭在野利用的微软 Exchange 服务漏洞、1 个遭在野利用的 IE 浏览器远程命令执行漏洞、多个 F5 BIG-IP 和 BIG-IQ 高危漏洞等，超过一半的高风险漏洞利用代码均已被公开。

（关注公众号“奇安信 CERT”，发送“202103”可查看 3 月需重点关注的漏洞完整清单）

政策篇

国内，行业网络安全政策、标准不断完善，《金融数据安全 数据生命周期安全规范》行业标准正式发布，为金融机构开展数据安全防护工作提供指导；国家医保局印发《关于加强网络安全和数据保护工作的指导意见》，提出了十四五期间医疗保障领域的网络安全发展目标和实现路径。

国际上，美国国家安全局计划发布非机密版 5G 安全指南，概述 5G 基础设施面临的威胁和风险，以帮助政府和行业将安全集成到 5G 生态系统的各个方面；欧盟理事会发布未来数字十年网络安全战略，将增强欧洲抵抗网络威胁的集体应变能力，强化网络安全领域战略自主能力。

国内

《金融数据安全 数据生命周期安全规范》行业标准正式发布

2021年4月8日，由中国人民银行科技司发起的《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）正式获批发布实施。《规范》规定了金融数据生命周期安全原则、防护要求、组织保障要求以及信息系统运维保障要求，在具体内容上分为 9 个部分，并附有数据采集模式、数据传输模式、数据脱敏等四个附录。《规范》建立了覆盖数据采集、传输、存储、使用、删除及销毁过程的安全框架，适用于指导金融业机构开展数据安全防护工作，并为第三方测评机构开展数据安全检查与评估工作提供参考。

国家医保局印发《关于加强网络安全和数据保护工作的指导意见》

2021 年 4 月 6 日，国家医疗保障局印发《关于加强网络安全和数据保护工作的指导意见》，要求落实网络安全主体责任，全面推进网络安全水平提升，实施数据全生命周期安全管理，为智慧医保建设、合法合规数据信息共享、多层次医疗保障体系建设提供有力支撑。《意见》提出，到 2022 年，基本建成基础强、技术优、制度全、责任明、管理严的医疗保障网络安全和数据安全保护工作体制机制。到“十四五”期末，医疗保障系统网络安全和数据安全保护制度体系更加健全，智慧医保和安全医保建设达到新水平。

交通运输部印发《交通运输政务数据共享管理办法》

2021 年 4 月 6 日，交通运输部印发《交通运输政务数据共享管理办法》，规范交通运输政务数据共享。《办法》提出，交通运输政务部门应遵循国家和行业网络安全管理法规、政策和制度，按照“谁管理、谁负责”和“谁使用、谁负责”的原则，建立健全政务数据安全保障机制，落实安全管理责任和数据分类分级要求，加强本部门政

务数据提供渠道和使用环境的安全防护，切实保障政务数据采集、存储、传输、共享和使用安全。

四部门联合印发《常见类型移动互联网应用程序必要个人信息范围规定》

2021 年 3 月 22 日，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局联合制定了《常见类型移动互联网应用程序必要个人信息范围规定》，明确移动互联网应用程序（App）运营者不得因用户不同意收集非必要个人信息，而拒绝用户使用 App 基本功能服务。《规定》对地图导航、网络约车、即时通信、网络社区、网络支付、网上购物、餐饮外卖、邮件快件寄递、交通票务、婚恋相亲等 39 类常见类型 App 的基本功能服务和必要个人信息范围作出详细规定，还首次将小程序纳入 App 收集个人信息的监管范围。

国际

美国国家安全局计划发布非机密版 5G 安全指南

据 Breaking Defense 4 月 7 日消息，美国国家安全局（NSA）执行董事 Wendy Noble 表示，NSA 正在和其他国家共同制定非机密版 5G 安全指南，预计将在春季发布。Noble 说，Noble 称，该指南汇集 NSA 在密码学和网络安全领域的专业知识，概述了 5G 基础设施面临的威胁和风险，以帮助政府和行业将安全集成到 5G 生态系统的各个方面。NSA 内部开发了数据分析方法，用来定义预期行为模式识别异常，实施零信任模型。该指南以持久安全框架 (Enduring Security Framework，ESF) 的研究成果为基础，ESF 是美国公私之间的具体合作框架，用于解决对美国国家安全系统和关键基础设施安全和稳定构成的威胁和风险。

美国政府发布容器安全指南，联邦机构需在半年内全部合规

据 GCN 3 月 16 日消息，美国联邦风险和授权管理计划（FedRAMP）今日发布《容器漏洞扫描要求》，介绍了 FedRAMP 计划内使用容器技术的云系统漏洞扫描中需要遵循的流程、架构及安全考虑等方面的特定合规要求。该文件确保了云服务提供商保持其容器技术合规，弥补了传统云系统和容器化云系统之间的合规差距。该文件给予了联邦机构和供应商 6 个月的合规时间。

欧盟理事会发布未来数字十年网络安全战略

据 Infosecurity Magazine 3 月 22 日消息，欧盟委员会正式发布未来数字十年网络安全战略的主要结论，该战略于 2020 年 12 月提出，旨在增强欧洲抵御网络威胁的能力，确保所有公民和企业都能安全使用数字工具和享受数字服务。战略指出，保障网络安全对于建设绿色和数字化的欧洲、实现战略自主权、增强欧盟的数字领导能力具有重要意义。作为塑造欧洲数字未来、欧洲复苏计划和欧盟安全联盟战略的重要组成部分，该战略将增强欧洲抵抗网络威胁的集体应变能力，并有助于确保所有公民和企业都能从可信赖和可靠的服务中充分受益。

政策解读

强制性国家标准《网络关键设备安全通用要求》合规要点

作者 汇业律师事务所顾问律师 史宇航

近日，强制性国家标准《网络关键设备安全通用要求》（GB 40050-2021）发布。《网络关键设备安全通用要求》是网络安全领域少数强制性标准之一，相对于推荐性国家标准更加值得关注。

一、网络关键设备的定义与范围

鉴于网络关键设备的特殊性，识别网络产品是否属于网络关键设备就成为了关键性的第一步。

根据《网络关键设备安全通用要求》3.7 中的定义，网络关键设备（critical network device）是指支持联网功能，在同类网络设备中具有较高性能的设备，通常用于重要网络节点、重要部位或重要系统中，一旦遭到破坏，可能引发重大网络安全风险。具体而言是指相关性能符合《网络关键设备和网络安全专用产品目录》中规定的范围的产品。

早在 2017 年 6 月《网络安全法》生效伊始，国家互联网信息办公室、工信部、公安部、国家认证认可监督管理委员会就联合发布了《网络关键设备和网络安全专用产品目录（第一批）》：

设备或产品类别	范围
1. 路由器	整系统吞吐量（双向）≥ 12Tbps 整系统路由表容量≥ 55 万条
2. 交换机	整系统吞吐量（双向）≥ 30Tbps 整系统包转发率大于等于 10Gpps
3. 服务器（机架式）	CPU 数量≥ 8 个 单 CPU 内核数≥ 14 个 内存容量≥ 256GB
4. 可编程逻辑控制器（PLC 设备）	控制器指令执行时间≤ 0.08 微秒

尽管四部委公布了目录，但目录中同一产品范围项下的不同门槛是“和”还是“或”并不清晰，需要实践中逐渐予以明确。另外随着技术的发展，后续四部委可能还会就网络关键设备和网络安全专用产品目录进行更新或扩充。

关于《网络关键设备和网络安全专用产品目录》的效力，在“张鑫、陈天明、张朝荣等提供侵入、非法控制计算机信息系统程序、工具案”中（（2018）浙 0602 刑初 101 号），浙江省绍兴市越城区人民法院进行过认定：

> 《网络关键设备和网络安全专用产品目录》公布的目的在于加强对网络关键设备和网络安全专用产品的安全管理，该目录项下的网络关键设备、网络安全专用产品类别须经过具有相关资质的认定机构按照国家标准的强制性要求进行安全认证后方可对外提供、销售，该目录的公布不具有规定“网络关键设备和网络安全专用产品是什么”或“目录之外均不属于网络关键设备和网络安全专用产品”的内在意旨，更非对“计算机信息系统安全保护措施”作出定义式限定。

因此，在关于网络安全产品销售的司法实践中，对网络关键设备和网络安全专用产品的认定可能会遵循更宽的尺度，需要在具体案件的实务中予以特别关

注。

二、法律义务

网络关键设备遵守国家强制性标准是一项重要的法律义务，《网络安全法》第23条明确规定：

> 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

概言之，网络关键设备的销售需要遵循以下流程：

《密码法》第26条也规定：

> 涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的机构检测认证合格后，方可销售或者提供。商用密码产品检测认证适用《中华人民共和国网络安全法》的有关规定，避免重复检测认证。
>
> 商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。

后续网络关键设备和网络安全专用产品目录的更新，可能会将更多的商用密码产品列入其中。

三、基本要求

在《网络关键设备安全通用要求》中主要分为“安全功能要求”与“安全保障要求”两个大类：

在合规的角度，《网络关键设备安全通用要求》不仅是开发工作中的具体要求，也可以作为合规工作中需要逐一勾选的清单。

在《网络关键设备安全通用要求》中，尤其值得关注关于运营和维护的要求，因为部分通信产品已经呈现出运维费用超过设备本身费用的现象，运维的质量甚至企业获取订单的关键要素，所以注定网络关键设备的销售不是“一锤子买卖”，需要关注网络关键设备运维的合规。而运维中最为敏感的就是远程运维，可能直接涉及到产品“后门”的问题，在《网络关键设备安全通用要求》中对远程运维有明确要求：

- 明示维护内容、风险以及应对措施；
- 留存不可更改的远程维护日志记录；
- 记录内容至少包括维护时间、维护内容、维护人员、远程运维的方式与工具；
- 获得用户授权并留存授权记录；并且
- 支持用户中止远程维护。

四、安全认证

网络关键设备的销售，除了符合强制性国家标准《网络关键设备安全通用要求》，还需要通过安全认证。早在2018年6月，国家认证认可监督管理委员会就发布了《网络关键设备和网络安全专用产品安全认证实施规则》。该规则将认证模式分为型式试验、工厂检查与获证后监督三个阶段：

- 型式试验采取抽检模式，一般每种产品抽样2套，如有特殊需求会增加样品数量。
- 工厂检查一般每个场所为2至6个人日，会重点关注：（1）标注的一致性；（2）生产场所产品与型式试

验产品的一致性；以及（3）是否违规使用认证标识。

· 获证后监督通常会以每年一次的频率进行，并且可能采取“飞行检查”的模式在不提前通知的情况下进行抽检。

设备通过安全认证以后，可以获得认证证书，有效期为5年。在通过认证产品的本体铭牌应加施认证标志，如果是软件产品，则应当在软件外包装或《许可协议》中显著加施使用标注。

根据2018年6月发布的《网络关键设备和网络安全专用产品安全认证和安全检测任务的机构名录（第一批）》，目前可以承担网络关键设备安全认证和安全检测任务机构包括：

机构名称	网址
中国信息安全认证中心	www.isccc.gov.cn
中国信息通信研究院 / 中国泰尔实验室	www.caict.ac.cn
国家计算机网络与信息安全管理中心	www.cert.org.cn
国家工业控制系统与产品安全质量监督检验中心	www.etiri.org.cn
中国电子技术标准化研究院赛西实验室	www.cesi.cn
工业和信息化部电子第五研究所	www.ceprei.com
信息产业数据通信产品质量监督检验中心	www.chinawllc.com
国家电话交换机质量监督检验中心	www.fritt.com.cn
信息产业无线通信产品质量监督检验中心	www.radio-qtc.com
信息产业有线通信产品质量监督检验中心	www.cdtr-lab.cn
信息产业光通信产品质量监督检验中心	lab.wri.com.cn
信息产业广州电话交换设备质量监督检验中心	www.mctc.org.cn

五、合规步骤与要点

根据我们的经验，网络关键设备合规工作可以从以下几方面入手：

1. 梳理产品目录

无论是对于网络设备的生产者还是相关领域的用户，都应当对自己生产或使用的产品进行梳理，判断是否有产品落入《网络关键设备和网络安全专用产品目录》的范围，对此类产品开展专项合规工作。

在此基础上，跟踪《网络关键设备和网络安全专用产品目录》的更新情况，一旦目录更新，及时调整自身的合规目录。

2. 产品合规

对于网络关键设备生产者，需要从设计环节伊始，就将国家标准的要求嵌入产品中。在功能与形式上达到国家标准的要求，并且通过文件让产品的合规性可以被验证。

对于网络关键设备的用户，也需要采购部门及时更新供应商名录，对网络关键设备的采购仅针对通过认证的产品开放。此外也需要网络关键设备用户的法务部门将国家标准《网络关键设备安全通用要求》落实到采购协议内产品质量相关的条款中。

3. 安全认证

对于网络关键设备生产者，通过安全认证是不可或缺的环节，需要及时申请、完成认证。在完成认证后，还应当在产品铭牌、包装或用户协议等合适位置准确进行标识。

除了应当完成安全认证并准确标识，网络关键设备生产者还应当做好安全认证通过后应对“飞行检查”的准备工作。网络关键设备生产者可以通过演练模拟飞行检查，帮助从前台接待到生产现场的每个环节做好准备，形成预案。

奇安信

新一代网络安全领军者

奇安信营销体系

招募精英

党政大客户部总经理

1.负责中央部委及二级单位市场的全年销售任务达成；
2.制定年度销售计划及预算，分解销售任务，推动并确保相应计划、目标的达成；负责团队的建设、管理、指导与激励；
4.重要客户中高层关系维护，项目运作与把握；潜在客户的市场拓展，制定增量目标，计划并达成；
5.进行市场调研与分析，研究同行业界发展状况，为公司战略制定、产品规划等方面提供相应建议。

大客户销售经理

党政/网信/电子政务/审计行业

1.根据公司及本行业销售任务开展销售工作，完成各项销售指标；
2.开拓、积累、夯实客户基础；
3.挖掘客户需求，为客户提供整体解决方案；
4.负责组织开展行业市场活动，加强公司在行业内的品牌影响力；
5.挖掘、反馈所负责行业的市场信息及客户需求，促进产品体系优化，构建有竞争力的市场策略。

售前技术专家

党政大客户部

1.负责国家党政机关头部客户的售前技术工作，协同党政大客户部销售拓展客户商机及业务布局，配合销售挖掘项目机会、引导客户需求
2.负责党政大客户部客户技术交流、项目技术文档编写、项目招投标等售前支撑工作；
3.负责党政大客户部技术策略梳理、技术资料整理，并能在党政机关头部客户进行技术和解决方案推广。

解决方案专家

党政/网信/电子政务/审计行业

1.协助行业技术负责人完成行业级解决方案、营销技术策略、行业技术资料整理，并能在行业进行技术和解决方案推广；
2.协同行业销售拓展客户商机及业务布局，配合销售挖掘项目机会、引导客户需求；
3.完成行业市场典型客户调研，不断提升解决方案竞争力，能洞察行业趋势、参与行业规范制定。

扫码联系我们

零信任之路

——新 IT 环境下的零信任架构建设与落地

作者 奇安信身份安全实验室 张泽洲

数字化转型及疫情推动的远程办公扩大了安全风险，“从不信任，总是验证”的“零信任”理念加速落地，成为解决云网边界消弭、重塑企业安全体系的的关键技术， 本期特别编辑新 IT 环境下的零信任架构建设与落地实践，希望成为建设方向选择的参考。

1 背景

数字化转型的时代浪潮推动着信息技术的快速演进，云计算、大数据、物联网、移动互联等新兴 IT 技术为各行各业带来了新的生产力，但同时也给企业网络基础设施带来了极大的复杂性。复杂的现代企业网络基础设施已经不存在单一的、易识别的明确安全边界，或者说，企业的安全边界正在逐渐瓦解，传统的基于边界的网络安全架构和解决方案难以适应现代企业网络基础设施。

另外，网络安全形势也不容乐观。外部威胁和内部威胁愈演愈烈，有组织的、武器化的、以数据及业务为攻击目标的高级持续攻击仍然能轻易找到各种漏洞突破企业的边界并横向移动，同时，内部业务的非授权访问、雇员犯错、有意的数据窃取等内部威胁层出不穷，成为数据泄露的重要因素。

业界需要全新的网络安全架构应对现代复杂的企业网络基础设施，应对日益严峻的网络威胁形势，零信任架构正是在这种背景下应运而生，是安全思维和安全架构进化的必然。

2 零信任架构及其核心组件

根据《零信任网络》一书，零信任架构的建立在以下设定之上：网络无时无刻不处于危险的环境中；网络中自始至终存在外部或内部威胁；网络的位置不足以决定网络的可信程度。因此需要：所有的设备、用户和网络流量都应当经过认证和授权；安全策略必须是动态的，并基于尽可能多的数据源计算而来。

NIST 在特别出版物《零信任架构》中指出，零信任架构是一种网络/数据安全的端到端方法，关注身份、凭证、访问管理、运营、终端、主机环境和互联的基础设施，认为零信任是一种关注数据保护的架构方法，认为传统安全方案只关注边界防护，对授权用户开放了过多的访问权限。零信任的首要目标就是基于身份进行细粒度的访问控制，以便应对越来越严峻的越权横向移动风险。

零信任的本质是在访问主体和客体之间构建以身份为基石的动态可信访问控制体系，通过以身份为基石、业务安全访问、持续信任评估和动态访问控制的关键能力，基于对网络所有参与实体的数字身份，对默认不可信的所有访问请求进行加密、认证和强制授权，汇聚关联各种数据源进行持续信任评估，并根据信任的程度动态对权限进行调整，最终在访问主体和访问客体之间建立一种动态的信任关系。

2.1 零信任关键能力

2.1.1 以身份为基石

基于身份而非网络位置来构建访问控制体系，首先需要为网络中的人和设备赋予数字身份，将身份化的人和设备进行运行时组合构建访问主体，并为访问主体设定其所需的最小权限。

2.1.2 业务安全访问

零信任架构关注业务保护面的构建，通过业务保护面实现对资源的保护，在零信任架构中，应用、服务、接口、数据都可以视作业务资源。通过构建保护面实现对暴露面的收缩，要求所有业务默认隐藏，根据授权结果进行最小限度的开放，所有的业务访问请求都应该进行全流量加密和强制授权。

2.1.3 持续信任评估

持续信任评估是零信任体系从零开始构建信任的关键

图 1 零信任架构的关键能力模型

手段，通过信任评估模型和算法，实现基于身份的信任评估能力，同时需要对访问的上下文环境进行风险判定，对访问请求进行异常行为识别并对信任评估结果进行调整。

2.1.4 动态访问控制

动态访问控制是零信任架构的安全闭环能力的重要体现。建议通过 RBAC 和 ABAC 的组合授权实现灵活的访问控制基线，基于信任等级实现分级的业务访问，同时，当访问上下文和环境存在风险时，需要对访问权限进行实时干预并评估是否对访问主体的信任进行降级。

2.2 零信任核心架构组件

零信任架构的关键能力需要通过具体的逻辑架构组件来实现，其逻辑组件参考架构如图 2 所示：

2.2.1 可信代理

可信代理是零信任架构的数据平面组件，是确保业务安全访问的第一道关口，是动态访问控制能力的策略执行点。可信代理拦截访问请求后，通过访问控制引擎对访问主体进行身份认证，对访问主体的权限进行动态判定。可信代理将为认证通过、且具有访问权限的访问请求建立安全访问通道，允许主体访问被保护资源。当访问控制引擎判定访问连接需要进行策略变更时，可信代理实施变更，中止或撤销会话。

2.2.2 动态访问控制引擎

动态访问控制引擎和可信代理联动，对所有访问请求进行认证和动态授权，是零信任架构控制平面的策略判定点。访问控制引擎持续接收来自信任评估引擎的评估数据，以会话为基本单元，秉承最小权限原则，对所有的访问请求进行基于上下文属性、信任等级和安全策略的动态权限判定，最终决定是否为访问请求授予资源的访问权限。

2.2.3 信任评估引擎

零信任架构中实现持续信任评估能力的核心组件，与访问控制引擎联动，持续为其提供主体信任等级评估、资源安全等级评估以及环境评估等评估数据，作为访问控制策略判定依据。

2.2.4 身份安全基础设施

身份安全基础设施是实现零信任架构的关键支撑组件，甚至可以说，零信任架构借助现代身份管理平台实现对人 / 设备 / 系统的全面、动态、智能的访问控制。身份管理和权限管理为访问控制提供所需的基础数据来源，其中身份管理实现各种实体的身份化及身份生命周期管理，权限管理实现对授权策略的细粒度管理和跟踪分析。

3 零信任产业发展现状

3.1 国外产业发展及国家战略

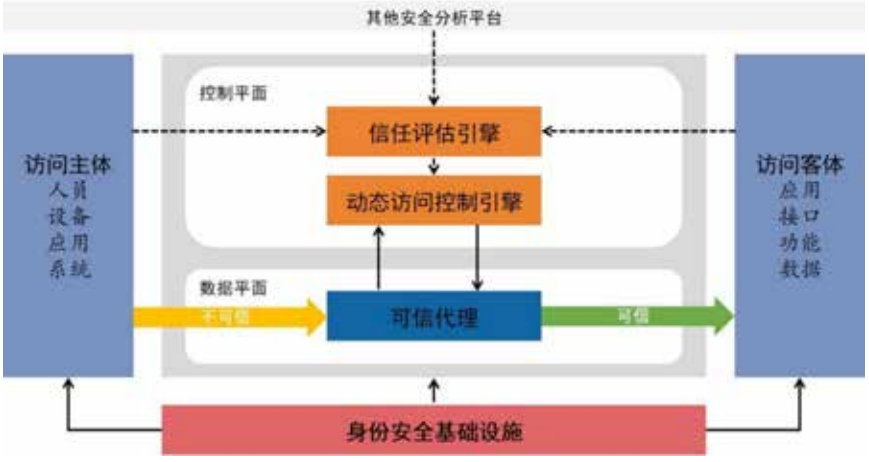


图 2 零信任核心架构通用参考架构

“零信任”这个词正式进入公众视野，距今已经过了 10 年时间。零信任在国际上的应用已经愈发广泛与深入：Google、Microsoft 等业界巨头率先在企业内部实践零信任，并先后推出可商业化的零信任产品与解决方案；Okta、Centrify、Ping Identity 为代表的身份安全厂商当仁不让，推出基于身份的零信任方案；Cisco、Akamai、Symantec、VMware、F5 等公司推出了偏重于网络实施方式的零信任方案；同时，零信任也催生了一批非常成功的创业公司，包括 Vidder、Cryptzone、Zscaler、Perimeter81 等。根据 Forrester2020 年二季度对于零信任产业的统计数据，按照零信任解决方案收入，将该市场的供应商分为大中小三类其中，其中零信任营收超过 1.9 亿美元的厂商已有 10 余家。

随着技术的成熟和产业基础的逐步完善，2019 年以来，美国军方、国防部、联邦政府和标准化组织纷纷发表各自的白皮书、评估报告和标准指南，阐述各自对零信任的认识、规划及落地方案。

DIB 作为美国国防部下属专注于技术与创新的机构于 2019 年 7 月发布了 DIB 零信任架构白皮书《零信任安全之路》，指导国防部网络实施零信任架构。紧接着在 2019 年 10 月发布报告《零信任架构（ZTA）建议》，建议国防部将零信任列为最高优先事项实施。这两个重量级文件的发布，反映出美国国防部对零信任的重要定位：零信任架构是美国国防部网络安全架构的必然演进方向。

作为联邦政府顾问智囊的美国技术委员会 – 工业咨询委员会（ACT-IAC），于 2019 年 4 月发布了《零信任网络安全当前趋势》白皮书。通过开展市场研究，评估了零信任技术成熟度和准备度、适合性、可扩展性和基于实际实现的可承受性，最终，对美国政府机构采用零信任提出评估建议。

2020 年 8 月 12 日，美国国家标准与技术研究院（简称 NIST）发布《零信任架构》正式版。该标准自 2019 年 9 月以来，先后发布两个草案版本，是迄今为止国际上第一个零信任架构指南文件。NIST 认为更多的组织 / 机构能够受益于零信任架构。通过提供多种零信任实现方式，NIST 希望 ZTA 不仅能在大型企业落地，同时在小型企业中也能发挥作用。不管采用何种方式实现，ZTA 应该围绕着企业本身的资产防护且遵守零信任原则宗旨进行，而具体的实现方式应充分结合企业现状。同时，风险评估也成为零信任的重要内容之一，企业如果希望向 ZTA 迁移，在考虑技术替代的同时，也要重视风险评估工作。

美国国家安全局（NSA）于 2021 年 2 月 25 日发布《拥抱零信任安全模型》网络安全报告。报告阐述了美国国防部（DoD）与其关联组织应如何建立零信任安全架构。网络安全专家能够通过部署零信任架构更高效地保护组织网络以及敏感数据的安全。该报告还介绍了零信任架构的优势及其潜在挑战，指出缺乏高层支持是组织无法大规模采用零信任的首要原因，并提出关于组织网络进行零信任架构实施的建议。此外，NSA 强烈建议将零信任安全模型部署到国防部中所有关键网络与系统。并且为充分发挥作用，零信任应在网络及其运营生态系统中大范围地实施。

零信任架构已经成为美国国家级安全战略，欧美地区都在加快零信任安全市场的布局与建设落地，可以说零信任已经进入规范化、规模化产业发展阶段。

3.2 国内零信任从概念走向落地

从国内情况来看，国家相关部门和业界对于零信任安全高度重视，零信任安全从概念走向落地。

工信部 2019 年起草的《关于促进网络安全产业发展的指导意见（征求意见稿）》提出，要积极探索拟态防御、可信计算、零信任等网络安全的新理念、新架构，促进网络安全理念和技术的创新。零信任安全首次被列入网络安全需要突破的关键技术，希望能够结合国内的应用场景，让零信任更好地落地发展。

2019 年中国信息通信研究院发布的《中国网络安全产业白皮书》中，首次将零信任安全技术和 5G、云安全等并列列为我国网络安全重点细分领域技术。

为了规范、引导零信任技术应用，国内同时在积极推进零信任的标准化进程。2019 年 7 月，在中国通信标准化协会 CCSATC8 WG3 第 60 次工作会议上，腾讯牵头提交的《零信任安全技术 – 参考框架》行业标准正式通过评审，成为国内首个立项的零信任安全技术行业标准。

2020 年 5 月，在全国信息安全标准化技术委员会 2020 年第一次线上工作组“会议周”上，奇安信牵头提出的《信息安全技术 零信任参考体系架构》，在 WG4（认证与鉴别组）工作组成功立项，这是零信任标准层面的首个国家标准，集合了相关企业、科研机构、高校、行业用户等多方角色参与标准规范编制，为零信任体系建设提供基础支撑和指导，具有重大作用和意义。

据安全牛研究报告《现代企业零信任安全构建指南》中显示，80% 国内用户认为零信任处于概念热度期，对运用零信任安全相关解决企业数据中心远程访问、云计算服务访问、边缘计算、5G、新兴互联网等场景下的安全问题充满信心；超过 80% 的调研用户表示有零信任应用计划。

市面上的零信任方案与创业厂商也如雨后春笋般出现。奇安信、腾讯、阿里、华为、深信服、启明等安全和互联网厂商都利用各自在安全领域的技术优势，推出了零信任整体解决方案，并积极寻找机会，开展全面应用实践；竹云、九州云腾等身份管理厂商积极推动身份管理技术在零信任架构上的应用；云深互联、蔷薇灵动、山石网科等厂商则积极推动 SDP、微隔离等零信任技术方案的应用实践。2019 年以来，我国相关部委、部分央企、大型集团、互联网企业都开始将零信任架构作为新建 IT 基础设施安全架构；银行、能源、通信等众多领域和行业针对新型业务场景，开展采用零信任架构的关键技术研究和试点示范。

4 零信任的典型适用场景

面向不同的应用环境、业务场景，零信任架构有多种灵活的实现方式和部署模式。面向远程访问、云计算平台、大数据中心、物联网、5G 应用等典型场景，按照访问主体和资源之间的关系，数据平面的访问代理重点考虑采用便于和被保护资源相结合的部署模式，如“设备代理 + 网关”模式、“资源门户”模式、“设备应用沙箱”模式等，搭建安全的访问通道，对访问请求进行分流。控制平面的访问控制引擎负责指挥，按照“先认证后连接”原则，建立、维持有效连接，实施对资源的安全访问控制。在此过程中，持续开展安全监控评估，对应用场景中出现的安全威胁及时响应，消减风险。

4.1 远程访问

远程办公已经逐步成为一种常态化的工作模式，这也是移动办公延展后的必然结果。在疫情的刺激下，全球开始了规模庞大的居家远程办公，据第三方调查数据显示，2020 年春节期间，中国有超过 3 亿人远程办公，以前在办公室开展的工作全部搬回了员工的家中。

而远程办公只是更为广泛的远程访问的一种形式，随着企业数字化转型，企业需要开放更多的业务给各种人员、各种设备、任何时间、任何地点的进行访问，除了远程办公，还有远程业务开展、远程运维、远程开发、合作伙伴远程访问等等。这种大量的、复杂的访问需求已经彻底打破了企业的物理边界，企业信息基础设施进入一种无边界化状态。

4.1.1 应用场景分析

在现在企业的信息化建设环境中，远程访问必须涵盖的应用场景越来越复杂：

（1）接入人员和设备的多样性增加

员工、外包人员、合作伙伴等各类人员，使用家用 PC、个人移动终端、企业管理设备等，从任何时间、任何地点远程访问业务。各种接入人员的身份和权限管理混乱，弱密码屡禁不止；接入设备的安全性参差不齐，接入程序漏洞无法避免等，带来极大的风险。

（2）企业资源暴露程度大幅度增加

企业资源可能位于企业内网服务器，也可能被企业托管在公有云上的数据中心；企业服务通常需要在不同的服务器之间交互，包括部署在内网、公有云、私有云中的服务器。一个典型的场景，公有云上的网站服务器与内网应用程序服务器通信后，应用程序服务器检索获得内网数据，返回给网站服务器。资源信息基础设施与应用服务之间的关系越复杂，引入的系统风险越高。

（3）数据泄露和滥用风险大幅增加

在远程访问过程中，企业的业务数据会在不同的人员、设备、系统之间频繁流动，原本只能存放于企业数据中心

的数据也不得不面临在员工个人终端留存的问题。同时，数据移动增加了数据“意外”泄露的风险，安全措施相对较弱的智能手机频繁访问企业数据也将对企业数据的机密性造成威胁。

4.1.2 先进性和创新性

近年来外部攻击的规模、手段、目标等都在演化，有组织的、武器化的、以数据及业务为攻击目标的高级持续攻击屡见不鲜。利用远程办公找到漏洞，突破企业边界后进行横向移动访问，成为最常见和最有效的攻击手段之一。

常见远程接入的方式主要有两种，一种是通过端口映射将业务系统直接在公网上开放；另一种是使用 VPN 打通远程网络通道。各组织都在对自己的安全边界进行“加固”，尽量使用 VPN 远程接入而非直接开放业务端口，增强威胁检测的能力等等。然而，这些手段基本上可以视作是传统的边界安全方案上的单点增强，难以系统性缓解远程移动办公带来的安全威胁。攻击者可以轻易利用弱密码破解或撞库，通过 VPN 进入内网，甚至可以利用 VPN 漏洞、业务系统漏洞直接进行渗透，突破企业边界，最终窃取有价值的数据资产。

零信任安全架构针对远程访问应用场景，不再采用持续强化边界的思维，不区分内外网，针对核心业务和数据资产，梳理访问这些资产的各种访问路径和场景，在人员、设备和业务之间构建一张虚拟的、基于身份的逻辑边界，针对各种场景构建一体化的零信任动态访问控制体系。主要包括以下创新点和先进性：

（1）构建更安全的远程办公网络

通过实施“从不信任并始终验证”，不同类型用户只能按照预先确定的信任级别，访问预先申请的企业资源，未预先申请的企业资源将无法被访问，阻止企业内部“漫游”情况。

（2）增强对企业应用和数据的保护

在实施“按需受控访问”的基础上，有效整合资源保护相关的数据加密、网络分段、数据防泄露等技术，保护应用资源、数据在网络中的传输和存储，并优先保护高价值资源。

（3）大面积减少攻击暴露面

用户通过访问认证之前，资源对用户隐身；即便在用户通过访问认证和授权，成功进入网络以后，零信任架构也将阻止用户漫游到未经授权的区域。零信任思维从根本上降低了外部（互联网可发现）和内部（内部威胁）攻击面。

（4）减少违规行为的影响

零信任架构中，用户只能按需获得有限访问权限，有助于限制违规操作、业务中断、安全漏洞等的危害范围和危害后果，降低了补救成本。

（5）缩减安全管理成本和潜在建设成本

零信任架构终结了安全防护手段各自为政的现状，在零信任架构实施时，可以通过与现有工具的集成，大幅度降低零信任潜在建设成本；零信任的“无边界信任”思想减少了 VPN 的使用，简化了运营模式，缩减了安全管理成本。

4.2 大数据中心

数字经济时代，数据是推动经济社会发展的必要生产要素，作为数据集中承载的数据中心，其重要性日益凸显。面对新基建的历史机遇，随着 5G 网络、人工智能、工业互联网等产业的成熟，移动互联网、物联网、工业互联网、

车联网等新型应用场景的持续推广带来数据指数级增长，海量数据进入数据中心进行集中存储和处理，对以数据中心为代表的计算基础设施提出了更高的要求。特别在过去一年的疫情常态化背景下，各大城市的科技防疫、远程访问、和电商消费等都离不开大数据中心的支撑，未来，随着社会对于数据处理能力的需求急剧增长，经济社会与人们日常生活将越来越依赖于大数据中心安全、稳定的运行。

4.2.1. 应用场景分析

大数据中心业务上要求数据集中与共享，一方面实现了多部门、多平台、多业务的数据融合；另一方面在数据中心内部打破了业务之间、部门之间的网络边界，实现互通互访。

大数据中心在实现数据的集中存储与融合的同时，也将集中更多的风险，从而使其更容易成为攻击的目标。大数据中心面临以下安全挑战：

（1）针对高价值数据边界的猛烈攻击

攻击者大量利用弱口令、口令爆破等惯用伎俩，在登录过程中突破企业边界、在传输过程中截获或伪造登录凭证。大型组织甚至国家发起的 APT 高级攻击，还可以绕过或攻破数据中心的访问权限边界，在数据中心内部进行横向访问。

（2）内部员工对数据的恶意窃取

在非授权访问、员工无意犯错等情况下，“合法用户”非法访问特定的业务和数据资源后，造成数据中心内部数据泄漏，甚至可能发生内部员工“获取”管理员权限，导致更大范围、更高级别的数据中心灾难性事故。

4.2.2. 先进性和创新性

目前大数据中心访问中东西向（内部）流量大幅度增加，而传统的安全产品基本都是在南北向业务模型的基础上进行研发设计的，在大数据中心内部部署使用时，出现诸如部署困难、运算开销太高，策略管理不灵活等问题。零信任架构通过微隔离技术，实现环境隔离、域间隔离、端到端隔离，根据环境变化自动调整策略，具有以下先进性和创新性：

（1）精细化隔离的网络安全策略

零信任通过关闭网络中的无用服务，消减网络结构（例如，不再采用 VLAN、子网、区域或 IP 地址等管理方式），改进策略创建过程，在不同等级的网络区域边界设置访问控制规则，建立扁平化的网络管理，真正实现精细化部署。

（2）以身份为基石的逻辑边界

零信任将用户、设备和应用程序组合作为访问主体，对访问主体进行身份鉴别和安全监测，并将其作为访问控制信任基础，保证身份可信、设备可信。同时，将访问主

体到大数据中心内部资源的连接进行隔离，建立细粒度访问权限控制，防止访问主体越权访问。

（3）安全策略自适应调整

基于业务之间的访问逻辑，快速发现内部不合规访问流量，为安全策略的调整提供决策依据。当数据中心发生变化时，通过策略分析引擎的计算，快速自动配置安全策略，加速安全工作流程，减少人为错误风险。

4.3 云计算平台

云计算以按需自助服务、泛在接入、资源池化、快速伸缩性与服务可计量为特征，同时，云计算作为基础支撑平台，参与角色复杂，包括云服务商、云服务客户、云审计者、云代理者和云基础网络运营者等。在过去十年，随着云计算技术的快速发展，云的形态也在不断演进。云计算快速发展带来“云边协同”、“云网融合”等云计算硬件和网络体系的结构重组，以容器、微服务、DevOps 为代表的云原生技术成为主流支撑技术。云平台特定技术引入的管理短板和技术瓶颈，使云平台面临极大安全威胁，成为发生网络攻击的重灾区。

4.3.1. 应用场景分析

云计算技术的快速发展带来了云平台的大量部署、应用和数据的大量迁移，在庞大复杂的云环境下，如何保证云系统资源安全，保证云服务提供商为云消费者提供安全诚信的服务，同时阻止非法用户对云资源的访问，成为云安全亟需解决的问题。云平台面临以下安全问题的挑战：

（1）云管理服务的安全性要求

未严格满足云管理服务的安全性要求会导致系统性风险。为保障云服务的安全性和可用性，通常云服务提供商会提供一组软件用户界面或 API，供客户用来管理云服务，实际使用过程中由于客户能力不足、意识不强等各种原因，这些安全功能往往形同虚设。此外，客户可能直接将应用程序转移到云中，云应用程序和影子程序共存情况下也会开放新的访问通道。

（2）共享技术漏洞带来的威胁

支持云服务基础设施的基本组件隔离程度不足，多租户架构或多客户应用的情况下，不同企业的系统彼此相邻，并且可以访问共享内存和资源，从而为攻击者创建了新的暴露面。

（3）云平台开源代码自身风险

云计算技术借助开源技术取得巨大发展的同时，也面临极大威胁。开源代码自身的开放性，也给了不法分子机会，例如针对容器基础设施的攻击在加速，不断有容器漏洞被利用的情况出现。

4.3.2. 先进性和创新性

云计算逐渐进入到重新定义服务模式的发展路径，专为云计算模型开发的云原生技术，涵盖一系列云计算技术体系和管理方法，可帮助用户快速将应用构建和部署到与硬件解耦的平台上。企业部署在云上的应用具备更高的敏捷性、弹性和云间的可移植性，广泛支持包括 Kubernetes、OpenShift、Docker EE、OpenStack 和裸金属服务等平台。随着越来越多的公有云上服务组件被使用，SaaS 安全也变得越来越重要，其中，用户最关注服务的身份认证、访问控制以及数据保护。在云计算中实施零信任访问控制，采用适配云计算平台、工作负载的技术，确保只有经过动态授权的工作负载才能运行、交互或进行数据访问。具有以下的先进性和创新性：

（1）实施细粒度的访问控制

零信任采用适用于虚拟机、容器、微服务等云平台组件的微分段策略，将网络策略和身份策略相结合，只允许数据在许可的系统和连接之间流动，并在不断变换的云环境进行更新时保持细粒度的访问控制。其中微分段策略不受虚拟、动态资产的物理位置限制。

（2）面向微服务的隔离机制

零信任基于微服务管理平台所提供的连接、安全、控制和观测模块，实现应用程序或服务隔离，帮助开发人员聚焦核心的业务逻辑，实施流量监控、负载匹配、访问控制和审计。

（3）“先认证后连接”的微服务

通过基于身份的验证和授权，对微服务间的访问进行鉴权，取得授权后在全链路采用双向 mTLS 进行加密，在集群中实现安全的服务间通信，通过自适应的访问控制来执行最小化的访问控制策略。

4.4 物联网

万物互联时代，5G、大数据、人工智能等新技术为物联网带来了创新活力，催生了智能家居、智慧车联、个人智能穿戴等新兴应用领域，衍生出繁荣多样的物联网业务，同时，物联网可以提供先前设备缺少的数据存储、网络连接以及计算功能，赋予设备新的效率和技术能力。在物联网越来越普及的同时，网络安全问题也甚嚣尘上。

4.4.1. 应用场景分析

物联网呈现出与传统网络不同的特性，其中海量多样化的物联网设备入网方式和自身弱点都带来无法忽视的系统风险。连接物联网的终端普遍存在自我保护能力弱，极易遭受攻击者恶意破坏的特点，在物联网发展如火如荼的同时，网络安全问题也逐步暴露出来。研究显示，利用木马、僵尸等手段针对物联网发动攻击的技术已经非常成熟，数以万亿感染的物联网终端，将会给智能家居、智能制造、智慧城市、工业互联网等物联网应用场景带来极大的风险。物联网面临以下安全问题的挑战：

（1）泛终端自身的安全短板

研究报告显示，攻击者越来越多地利用智能家居传感器、智能手机、路由器上的各种漏洞将其作为新的攻击媒介，物联网终端已经成为事实上的攻击“跳板”，将安全威胁带入全网。根据银行业的最新安全警报，出现通过生物识别终端，发动对金融机构供应链攻击的案例，泛终端自身漏洞导致的安全风险防不胜防。

（2）多样化终端接入管理困难

随着物联网的广泛使用，物联网设备快速兴起，传统的哑终端、非智能终端也开始向智能终端靠拢。数量众多、类型多样、不同接入方式的泛终端，既需要传统的网络准入控制、企业资源管理等产品对办公终端进行接入管理，也需要统一终端管理等产品对移动端和服务器进行接入资产管理。同时，对于物联终端，尤其是在传统 PC 终端、移动端混合接入的场景下，还面临接入认证和管理的难题。

（3）物联终端攻击易于成功

物联网终端采用多样化接入技术，包括2G/3G/4G/5G、WiFi、蓝牙、Zigbee、LoRa、NB-IoT等，在云网融合背景下，5G 物联网装置绕过了中央路由器直接接入 5G 网络云端。由于物联网终端具有数量巨大、安全防护能力较弱等特性，在安全管控措施不到位的情况下，高级攻击者利用设备的脆弱性，从内部攻击服务平台，将更容易获得成功。

4.4.2. 解决思路

随着边缘计算技术的不断完善，边缘计算在本地执行计算和分析的思想也越来越被接受，云边协同成为新的基础架构，极大地满足物联网大部分场景在敏捷连接、实时业务、数据优化、安全与隐私等方面的计算需求。在物联网实施零信任架构，可借助边缘计算技术，解决终端的身份认证和访问控制，允许身份可信、经过动态授权的物联设备入网，并动态监测，及时发现并处置假冒、伪造的非法连接。

（1）部署边缘物联接入管理设备

在物联设备接入侧部署边缘物联接入管理设备，接管物联设备的身份管理、权限分配、接入控制等接入管理功能，物联接入管理设备和数据中心联动，在网络边缘处协同使用计算、连接、存储能力，及时处理物联设备相关请求，控制安全风险范围。

（2）建立物联设备标识管理机制

面对物联终端主要存在的终端设备仿冒、用户身份仿冒问题，根据物联终端各自不同的特性，可以采用不同的身份标识实施身份鉴别。高可信设备采用可信芯片 + 可信 OS，直接标识身份；嵌入式设备采用设备标签，如移动设备识别码（IMEI）、应用开发商标识符（IDFA）、唯一设备标识码（UDID）等，以及设备外贴 RFID 电子标签、密码模组等，都可以帮助建立设备身份标识；对于智能程度较低的物联设备，也可以采用设备数字指纹的方式来构建设备标识，解决设备入网身份管理问题。

（3）建立物联设备安全基线库

采用灵活的方式，对物联设备建立安全基线。在物联设备标识管理基础上，综合获取物联设备信息，包括操作系统类别、操作系统版本、涉及敏感数据的 App 特征、业务访问记录、行为特征等，运用人工智能深度学习等技术手段，建立安全基线库，帮助快速精准判断设备运行环境是否正常，及时发现被“攻陷”设备。

零信任方案实践案例

案例 1：某银行构建安全高效终端远程访问模式

随着某银行业务发展以及数字化转型的需要，远程办公成了不可缺少的办公手段，并日渐成为该行常态化办公模式。同时，经过新冠肺炎事件影响，使得行内有些业务必须对外开放远程访问。

该行远程访问存在三个主要安全风险：1）远程访问使用的设备存在安全隐患。

2）VPN 和云桌面自身存在安全漏洞，尤其是 VPN 极易成为渗透内网的跳板。3）静态授权机制无法响应风险。发生用户的异常操作、违规操作、越权访问、非授权访问等行为时，无法及时阻断访问降低风险。

通过部署和使用零信任远程访问方案，该银行已经实现了：业务隐藏、收缩暴露面；终端检查、确保终端环境安全；持续验证、提升身份可信；按需授权、细粒度访问控制；安全加固，防止设备被打穿。

该银行成功构建了安全、高效和合规的终端远程访问模式，实现了以最小信任度进行远程接入，对应用权限的

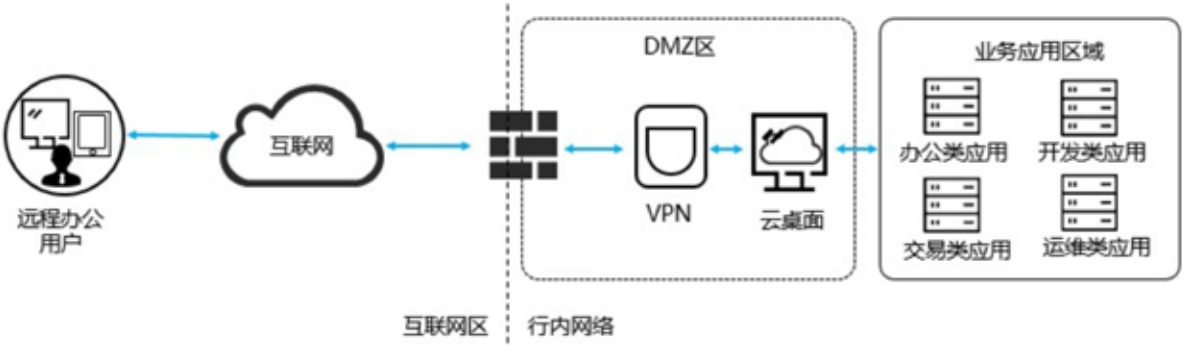


图 3 某银行远程办公场景

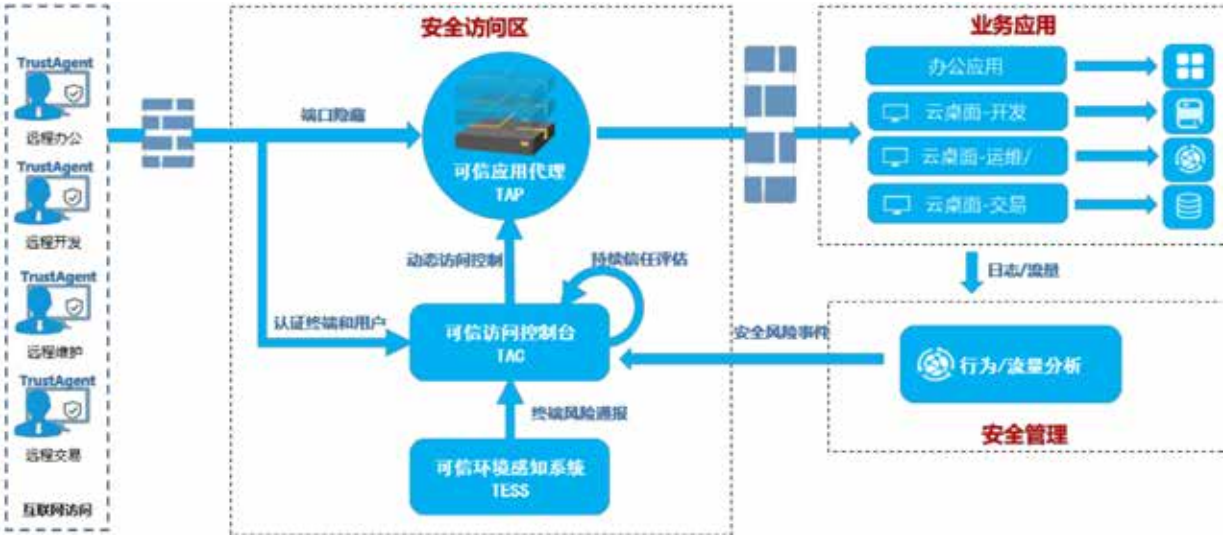


图 4 某行零信任远程访问方案架构

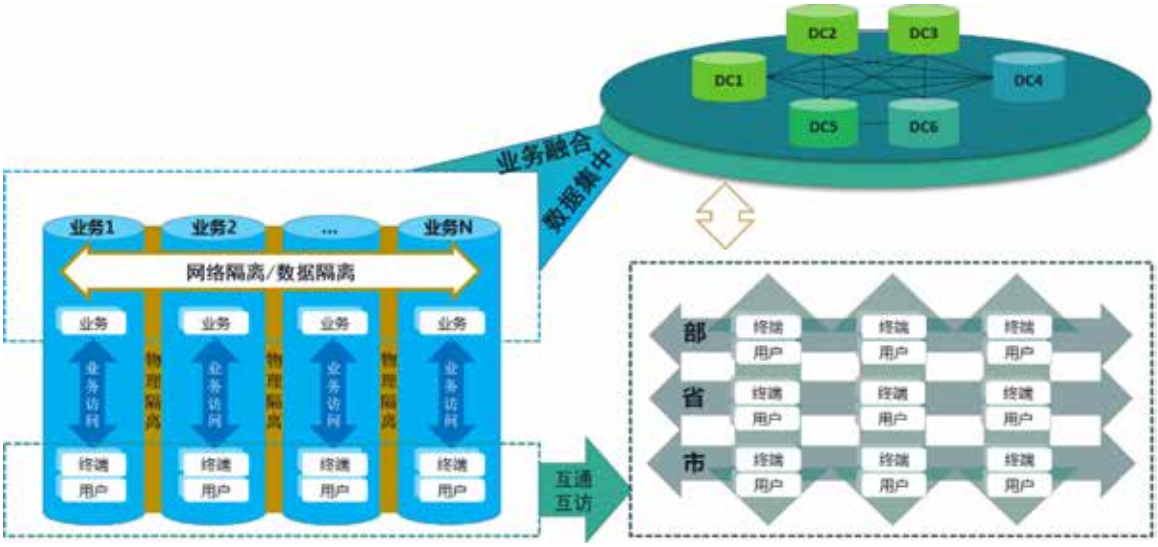


图 5 大数据中心安全场景

“最小授权”，企业数据的安全传输，达到了远程访问的动态访问目的。同时，无缝对接现有云桌面，保护云桌面安全接入，支持多类型 BYOD、CYOD 远程接入支持，不再受限于办公终端。

案例 2：某大型部委大数据中心访问安全

某大型部委业务覆盖部、省、市、县等多级行政机构，面临数据共享开放，交叉使用的场景，大数据应用面临的安全威胁和攻击种类多，攻击行为具有隐蔽性、攻击特征变化快，依赖传统信息安全防护技术来防范大数据攻击存在局限性，这主要是因为：(1) 数据集中导致安全风险增加；(2) 基于边界的安全措施难以应对高级安全威胁；(3) 静态的访问控制规则难以应对数据动态流动场景。

为应对上述安全挑战，该部委基于零信任架构构建安全接入区，在用户、外部应用和大数据中心应用、服务之间构建动态可信访问控制机制，确保用户访问应用、服务之间 API 调用的安全可信，保障大数据中心的数据资产。通过零信任体系架构的部署和使用，实现了业务流量强制加密，避免用户侧信息泄露，对业务应用进行了隐藏，从应用、接口层面收缩大数据对外暴露面。实现了用户流量不直接进入数据区，避免恶意流量渗透数据中心。对人员、终端、业务 / 数据、安全策略一体化动态访问控制，满足用户远程访问、数据交换两类安全需求。

案例 3：某大型企业实现终端数据隔离

某世界级通信行业企业，面临全球多分支机构、多用户类型，网络环境复杂，终端数据保护、防泄漏与用户访问的安全能力是焦点。过去该企业通过云桌面方式进行数据保护，成本高、网络需求复杂，同时很难对终端落地数据资料进行加密及管控。用户期望可以实现员工终端访问不同的业务资源且业务数据落地后安全，同时保证访问业务资源时用户身份安全、网络环境可信。

项目通过零信任安全解决方案，实现用户身份校验、网络环境可信检测、网络接入隔离、容器中进程隔离、容器存储加密等安全能力，有效预防终端数据落地，对数据访问流量实现了全程控制。

项目以基于沙箱的容器实现终端数据保护和业务访问控制，针对不同用户、不同业务、不同网络的访问控制需求和数据保护能力。实现了用户业务数据分级存储，安全策略统一控制，业务数据安全传输，强制加密，确保了业务数据传输安全。

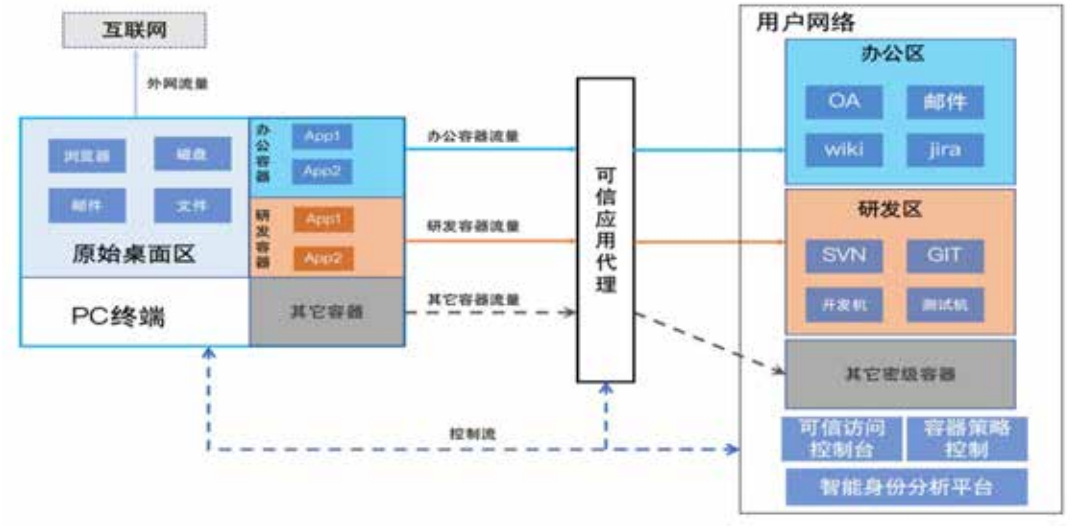


图 6 基于沙箱容器的终端数据保护和业务访问控制

案例 4：某银行构建安全高效特权访问环境

随着某银行客户的大数据智能化建设不断推进，数据在汇聚、共享和应用过程中存在巨大安全风险：在客户网络环境中，有大量的服务器、虚拟机和网络设备，但并无配置管理数据库（CMDB）/ 堡垒机等设备对特权账号统一纳管，所有的账号信息目前几乎都是以明文台账的形式保存在内部管理员或者厂商负责人的电脑中，甚至有的口令是明文存储在厂商的 SVN 仓库中让员工共享；账号的分发使用同样是以明文的方式提供给使用者，未做任何保护。

通过部署和使用开发测试与运维方案，银行构建了安全、高效和合规的特权访问环境，有效抵御恶意的外部入侵和内部威胁。通过零信任动态访问控制，实现全方位地管理特权账号和特权会话，帮助该行保护敏感信息和关键资产；实现对特权账号全生命周期的管理，自动改密可简化工作流程，从而提升工作效率，降低运维成本；详细记录特权账号活动记录和特权操作行为记录，便于管理员重溯操作取证定责，同时满足行业法律法规要求。

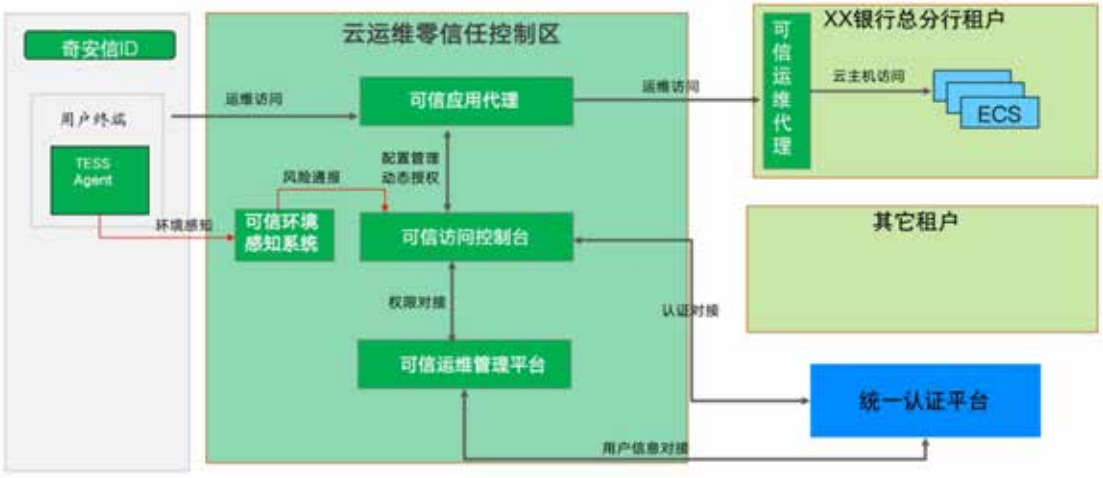


图 7 某银的安全、高效和合规的特权访问环境

案例 5：某市政务云访问安全

某市政务服务云化升级改造，业务系统集中上云，各委办局业务资源整合，进行统一纳管，面临众多问题：业务接口对外开放，面临数据访问安全问题；应用资源暴露面增加，安全风险加大；同时业务访问终端分散，设备安全性、合法性问题突出；用户侧业务访问权限控制固化，无法进行自适应安全控制。

用户在数据域和用户域之间建立零信任安全访问平台区域，实现统一安全接入、单点登录等。实现了业务集中代理，应用系统对外隐藏，业务端口收缩；通过环境感知服务实现各委办局访问终端风险情况实时感知，感知结果实时上报，重新评估主体信任，动态调整访问权限；同时建设了统一认证入口，实现了业务系统的单点登录。

某市政务服务云通过建立零信任安全访问平台，实现了业务整合上云，实现了资源集中安全防护，提高了管理效率，同时搭建的一体化安全访问平台，满足了多种类型架构应用，资源防护全覆盖。平台综合多维度风险信息，基于身份评估的动态访问控制机制，实现各委办局办公安全接入。

零信任迁移方法论

零信任架构作为一种全新的安全架构，和企业现有的业务情况、安全能力、组织架构都有一定的关系，零信任迁移不可能一蹴而就，需要遵循一定的方法论，结合企业现状，统一目标和愿景后进行妥善规划并分步建设。

零信任迁移方法如图 8 所示：

6.1 确定愿景

零信任的建设和运营需要企业各干系方积极参与，可能涉及到安全部门、业务开发部门、IT 技术服务部门和 IT 运营部门等。企业数字化转型的关键决策者应该将基于零信任的新一代安全架构上升到战略层面，确定统一的愿景，建议成立专门的组织（或虚拟组织）并指派具有足

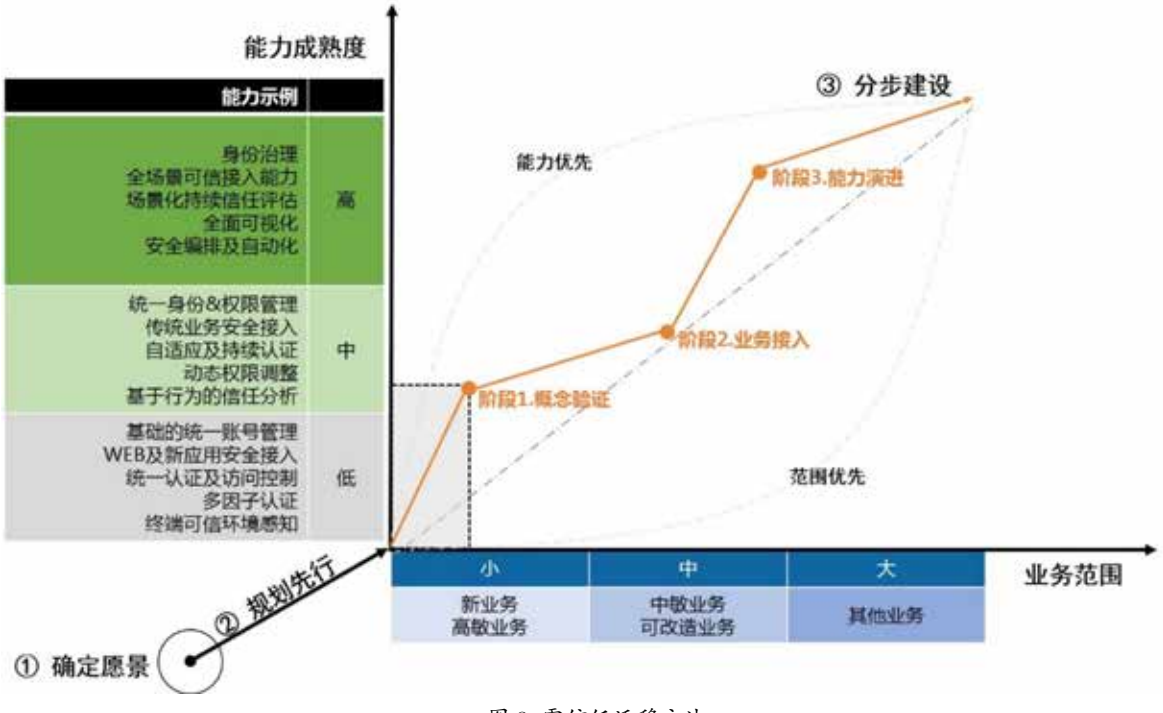


图 8 零信任迁移方法

够权限的人作为负责人进行零信任迁移工作的整体推进，建议至少由 CIO/CSO 或 CISO 级别的人员在公司高层决策者的支持下推动零信任项目。

需要特别注意的是，在很多企业安全部门话语权并不高，安全项目往往受到业务部门的阻碍甚至反对，零信任项目的发起者一定需要从零信任的业务价值出发，说服业务部门和公司的高层决策者。

另外，在零信任的迁移过程中，需要更多部门和人员的配合和支持，特别是大量的普通员工，他们作为零信任项目的最终使用者，他们的支持至关重要，建议通过公司级的持续的安全文化活动加强全体人员对零信任安全的认可，这一点也至关重要。

6.2 规划先行

零信任架构是安全思维和安全架构进化的必然，聚焦身份、业务、信任和动态访问控制等维度的安全能力，而这些能力业务密不可分，所以零信任天生就应该是一种内生安全。零信任的建设路径需要结合现状和需求，将零信任的核心能力和组件内嵌入业务体系，构建自适应内生安全机制，建议在业务建设之初进行同步规划，进行安全和业务的深入聚合。

规划的目的在于厘清形状，确定路径。对于零信任架构而言，需要从两个维度进行梳理和评估，一是能力成熟度维度，一是业务范围维度。

零信任架构的关键能力包括：以身份为基石、业务安全访问、持续信任评估和动态访问控制，每一项关键能力又可以划分为若干子能力，企业需要评估当前具备的安全能力，并基于风险、安全预算、合规要求等信息，确定安全能力建设的优先级。

零信任架构最终需要覆盖企业的所有资源，为其构建保护面。企业资源包括但不限于：应用、接口、功能和数据等。在规划阶段，需要确定迁移至零信任的业务优先级。一般来说新建业务和核心业务作为第一优先级考虑。

对安全能力现状、需求，业务现状、优先级进行梳理后，需要进一步对核心业务的暴露面进行梳理，对各暴露面的访问主体、访问主体的权限进行梳理，确定初步的总体建设路径及第一阶段建设方案。

6.3 分步建设

规划完成后进入建设阶段，根据规划的思路导向，建设阶段的划分依各企业而各有不同。如果是能力优先型建设思路，需要针对少量的业务构建从低到高的能力，通过局部业务场景验证零信任的完整能力，然后逐步迁移更多的业务。范围优先型则先在一个适中的能力维度上，迁移尽量多的业务，然后再逐步对能力进行提升。两种建设思路各有侧重，依据企业的具体情况，在规划阶段选定思路和建设阶段的划分。

一种建议的分步思路主要包含三个阶段：概念验证、业务接入和能力演进。首先在一个较小业务范围内，构建中等的零信任安全能力，对整体方案进行验证；方案验证完成后，对验证过程的一些局部优化点进行能力优化，并同时迁入更多的业务进一步验证方案并发现新的安全需求；最后，基于验证结果规划后续能力演进阶段，逐步有序的提升各方面的零信任能力。

零信任架构作为一种全新的安全思路，是持续演进的过程，需要基于业务需求、安全运营现状、技术发展趋势等对零信任能力进行持续完善和演进。

7 结语

零信任不应是某个短跑比赛，而是一场马拉松。疫情极大地改变了企业的工作方式，并且迫使很多企业和组织加快了数字化转型和改变安全战略。一个真正有效的零信任解决方案，应该帮助企业达成零信任安全效果的同时改善员工体验，而不是成为阻碍业务发展的另一种外挂式安全工具。零信任作为一种内生安全机制，落地过程中要始终用体系框架，从工程化思维去指导和推动。首先需要深入理解零信任的能力，关注零信任各项能力的平台化联动与打通，并场景化构建零信任参考技术架构和安全运行规程。零信任的落地建设需要通过工程体系进行管理和推动，规划先行，分步建设。将零信任能力和架构与目标运行环境进行聚合，将安全能力内生到各业务场景，实现为企业的数字化转型保驾护航。安

奇安信
新一代网络安全领军者

“天眼+安服”创新安全运营服务

奇安信 新一代网络安全领军者

奇安信融合自身的优势资源，推出了“天眼+安服”的安全运营服务。通过本地部署“天眼新一代威感知系统”检测网络中的各类安全威胁，再结合专家级的安全分析服务，有效应对高级持续性威胁（简称APT），为政企客户提供优质的安全运营服务。

目前“天眼+安服”的安全运营模式已经在政府、金融、能源、教育等诸多行业当中应用，并得到了广泛认可。在未来1-2年，随着各种新型攻击的持续发生，该模式将成为政企高级威胁防护的主流。

奇安信
新一代网络安全领军者

www.qianxin.com
kefu@qianxin.com
4009-303-120

奇安信
新一代网络安全领军者

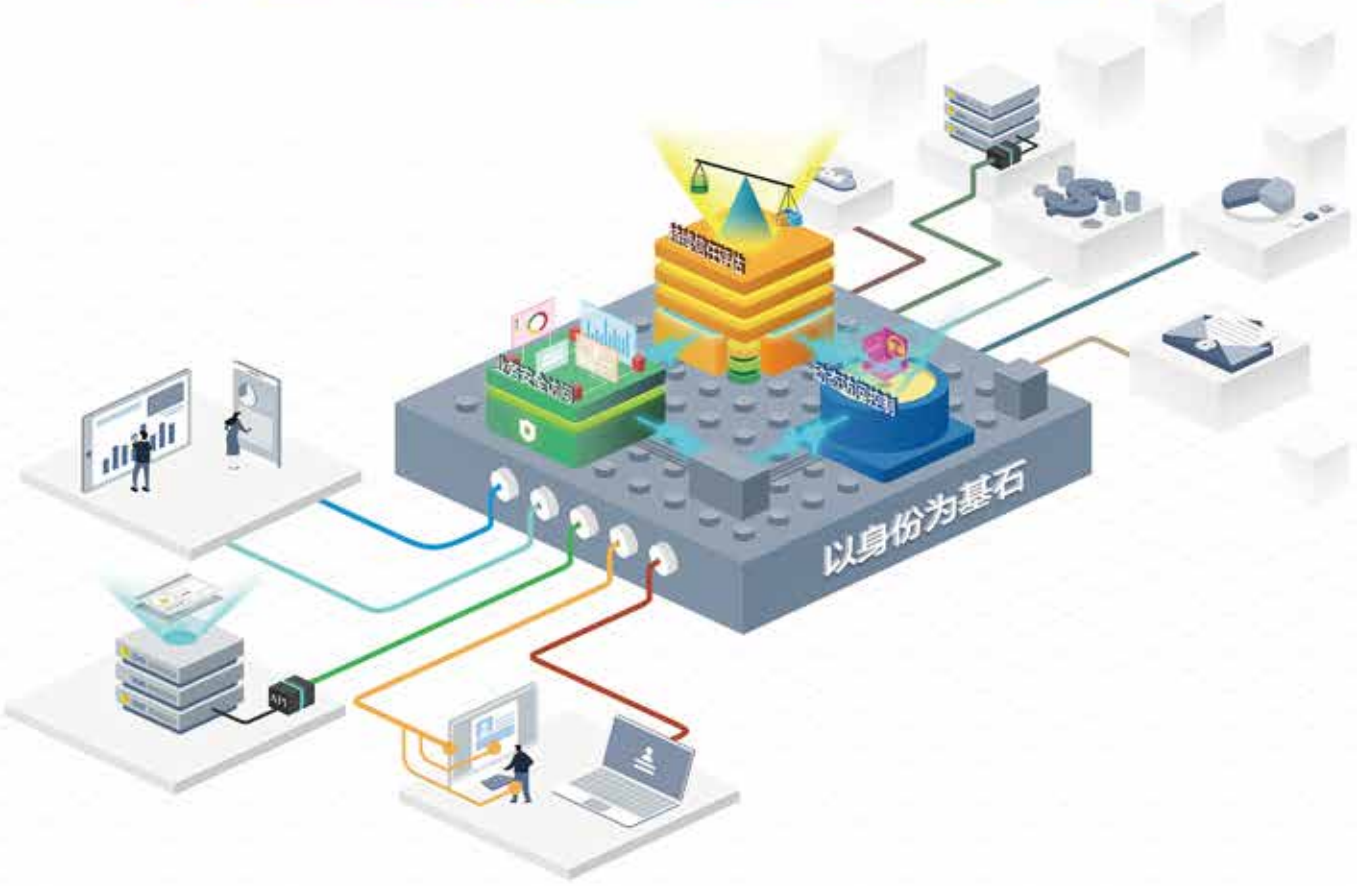
让网络更安全 让世界更美好

云计算和大数据时代

网络安全边界逐渐瓦解，内外部威胁愈演愈烈

传统安全架构正在失效

零信任安全 新身份边界



以身份为基石

- 为人和设备赋予数字身份
- 为数字身份构建访问主体
- 为访问主体设定最小权限

业务安全访问

- 全场景业务隐藏
- 全流量加密代理
- 全业务强制授权

持续信任评估

- 基于身份的信任评估
- 基于环境的风险判定
- 基于行为的异常发现

动态访问控制

- 基于属性的访问控制基线
- 基于信任等级的分级访问
- 基于风险感知的动态权限

构筑基于身份的动态虚拟边界

全面身份化 | 授权动态化 | 风险度量化 | 管理自动化

www.qianxin.com
kefu@qianxin.com
400-930-3120

捕获一段攻击代码之后，她发现了一款安全软件的“安全危机”

世界上没有任何一款软件是绝对安全的，网络安全软件也不例外。
——题记

作者 公关部 魏开元

2021 年 2 月 10 日，农历腊月二十九，当所有人都已经沉浸在了放假的喜悦中时，公司的终端安全软件突然弹出一个告警窗口：补安软件（某安全软件化名）正尝试启动 xx 程序，是否允许?

正在收拾行李的水子哥抬头看了一眼电脑屏幕，还没来得及细看告警详情，就直接点击了允许按钮。“应该是安装哪个补丁误告警了吧。”水子哥心想，为了让这个春节假期过得舒坦点，网络安全部这几天做了完善的补丁安装计划，针对可能被攻击者利用的脆弱点和暴露面进行修补，这会儿已经快装完了。

“等进度条 100% 了就撤吧。”水子哥对网络安全部的同事们说，“过去一年大家都辛苦了，老加班，黑客也不消停，明晚给大家一人发个大红包。”

“老大万岁……”

几条异常的 DNS 解析记录，形迹可疑

当晚九点半，绝大多数“打工人”都已经离开了写字楼，不过在奇安信安全中心，几条奇怪的 DNS 解析记录，吸引了美女分析师佳佳的注意。

“威胁雷达的检测模型发现了几次异常的 DNS 解析

请求，有点不太对劲，应该是咱们的客户。”佳佳对一旁的 DP 师傅说。

DP 凑过头来一看，说：“你在我们 Alpha 威胁分析平台上查一下目的 IP，看看有没有恶意标记”

“我查过了，没有标记，但是从行为来看非常可疑。保险起见的话还是应该通知销售，让他们联系客户尽快排查一下，看看是不是哪台机器中了木马。”佳佳说出了自己的担忧。

“行，不过要是真中招了，这七天假就过不安生了。”DP 打趣道，顺手给负责这个客户的销售发了一条语音消息。

接到销售电话后，水子哥觉得相当郁闷，怎么偏偏刚一放假就可能出事儿了。“你们能派两个专家来现场帮忙排查一下么，争取明天上午就能有个初步结果，这大过年的我们人手不够……”水子哥小心翼翼问了一句。

“我得先和我司威胁情报中心的威胁分析师商量一下，估计问题不大。”

“那太感谢了。”水子哥回应。

紧接着，这名销售就拨通了佳佳的电话，转达了客户的需求。本来销售还有点不好意思，但还在公司排查 DNS 日志的佳佳倒是很痛快的应承了下来：“明天上午九点，我跟 DP 师傅过去看看。”

捕获攻击代码，证据确凿

“来啦，这大年三十儿的真不好意思，中午我请客。”看到佳佳和 DP 过来，水子哥连忙迎上去，“你们来之前，我重点在排查最近一个月的告警，目前还没有发现什么问题。”

“嗯。要不您先休息会儿吧，黑眼圈都出来了，接下来交给我们就行。”话音未落，客户侧部署的奇安信态势感知与安全运营平台（简称 NGSOC）产生告警，疑似检测到网络攻击，并且捕获到了攻击代码。

“呵，基本没跑了，威胁情报匹配显示，攻击载荷（payload）来自于海莲花组织。”佳佳看完告警信息说到。

事实上，这不是水子哥他们单位第一次遇到有关海莲花组织的告警。早在去年 9 月，NGSOC 就已经产生过类似的告警，当时网络安全部的同事直接把攻击 IP 给

封禁了，并没有发现有什么其他异常情况。

听完水子哥的介绍，结合 NGSOC 刚才的告警信息，佳佳立刻有了初步的判断：第一，海莲花组织攻击的时间线较长，甚至可能要早于去年九月；第二，内网应该有多台办公终端被植入远控木马，需要完成定位。

考虑到应尽快拿到木马样本，佳佳决定从终端安全软件的日志开始排查，毕竟木马是直接运行在终端上的。

这一查，倒是让佳佳两人小小的意外了一下：昨天的日志显示，补安软件启动了一个未知程序，这个程序很可能就是海莲花组织植入的远控木马。

这个补安软件也是一款较为流行的桌面管理软件，水子哥他们公司主要将该软件用于补丁分发，是安全运营中非常重要的一环。这么看来，如果木马实锤了，那么海莲花组织很可能是攻破了补安软件服务端，并利用该软件下发远控木马。

顺着这条线索，佳佳很快在一台主机的 C 盘目录下，找到了该程序，并将其放到云沙箱运行。不一会儿，沙箱运行结果出来了。

“重大发现！”佳佳对正在排查 NGSOC 告警的 DP 师傅说，“补安软件昨天启动了木马程序。”

话音未落，一旁的水子哥瞬间不淡定了：“不是吧，就这么倒霉？”

DP 师傅倒是没有接茬，而是专心分析捕获的那段攻击代码。从运行结果来看，这段代码的主要目的应该是远程修改办公终端的登录口令，但由于捕获到的代码并不完整，没有办法推断攻击者的完整意图。

好在已经发现了补安软件的异常行为，接下来应该可以通过排查补安软件服务器端的日志，尝试补全这段攻击代码。

借助 NGSOC 提供的海量日志关联分析能力，佳佳他们很快补全了 EXP，并且还原了攻击者的入侵轨迹：海莲花组织首先攻破了补安软件的服务端，利用服务端的统一管控功能，修改部分办公终端的登录口令，向其下发木马程序。

让他们都没想到的是，分析结果显示，此次攻击最早可能发生在 2020 年 7 月中旬，海莲花组织就已经入侵了财务专用电脑，并且 NGSOC 已经产生告警。但由于当时安全运营人员忽略了这条告警，并且木马活动的日志也已经被删除，佳佳他们并没有发现更多有用的信息。

二十一台失陷终端，无一漏网

“佳佳，这个事情你怎么看？”DP 师傅不禁问到。

“用眼睛看。”佳佳打趣说，根据以往应急响应的经验，大型甲方客户的安全运营人员一天可能会收到成千上万的告警，如果缺乏有效的告警运营手段和自动化工具的辅助，其工作效率必然不会太高。为了处置看起来优先级更高的告警，部分告警往往会被忽略。

况且潜伏了这么长时间，失陷的办公终端恐怕不在少数。另外风险源头得尽快查清楚，不然下次攻击的到来估计不会太久。

说话间已到中午，水子哥自掏腰包，带着二位来到公司楼下最有牌面的饭店吃饭。

“对了，攻击 IP、URL 还有木马程序各个组件的特征都提取了没有，先尽快排查都哪些终端失陷了吧。”水子哥提了一嘴。

“这您放心，此次攻击所使用的失陷检测情报 IOC（包括恶意 IP、URL、木马程序的文件签名等）我们基本提取完了，一会儿吃完饭您更新一下终端安全软件的病毒特征库，再把所有内网终端查杀一遍。”佳佳放下筷子，又补充了一句，“这次木马样本免杀做的不错，终端杀毒软件没有报毒也能理解。或者您不妨试试我们奇安信天擎，误报、漏报方面都能控制在非常低的水平。”

哈哈哈哈，在座的三位都笑了，这广告打的猝不及防。

吃过饭后，水子哥三人三步并作两步回到了他们单位，尽快排查所有失陷的终端：配置好新规则的终端安全软件一丝不苟地翻着每一台电脑的每一个文件夹；另一边，佳佳则和 DP 师傅重点查 DNS 日志，看看哪些终

端连接了海莲花组织所使用的 IP 地址和 URL。双管齐下，绝不让一台被木马感染的终端漏网。

临近下午四点，21 台失陷终端全部被找出。

“太感谢了。”水子哥激动地表示，“晚上就不留你们了，你们还要团年呢。另外，下午我已经把这个情况反馈给补安软件供应商了，他们说尽快排查风险。”

临走之前，佳佳给水子哥留下了一条建议，风险修复之前，先关闭补安软件服务端。至少在春节期间，影响也不大。

拉网式排查 挖出多个安全隐患

晚上 8 点钟，在吃完两个人的年夜饭之后，佳佳的思绪又短暂的回到了这次 APT 攻击上。“海莲花组织到底是利用什么方法拿下了内网补安软件服务端呢？是 0day 漏洞吗？还是别的什么？”种种疑问，目前尚不得知，还需要进一步的排查。

大年初一早上十点来钟，一阵急促的鞭炮声，吵醒了熟睡中的佳佳。洗漱完毕后，她拿起手机一看，大概半小时前 DP 师傅发来了一条信息：还没起吧？水子哥说补安软件公司的人已经到他们公司现场去排查了，问我俩有没有时间，十一点钟过去一起看看，你要是不想去的话我一个人去也行。

“正合我意！”佳佳心道，看着桌子上早已摆好的热腾腾的饺子，她迅速吃了一碗，便打车出门了。

有了补安软件供应商的帮助，这次的排查开展的相当顺利，不到两个小时的时间，佳佳他们就已经发现了一个重大漏洞：由于某次版本更新时，程序员将一个非常重要的循环语句的返回值写错了，导致了在满足特定条件时，内网任意一台终端都可以通过访问补安软件，向另外一台终端下发指令，这与原来只允许通过服务端下发指令的设计初衷严重不负，存在非常大的安全隐患。

这意味着，黑客组织只要登录内网任意一台终端，便能向其他所有终端进行横向渗透。经版本追溯，这个漏洞已经存在了三个版本，时间跨度达半年之久，这让在场所有工作人员都吃了一惊。

“交给你们了。”DP 师傅对着一旁补安软件的人说，“我们先撤了啊。”

“等等，我觉得还是不太对，就目前的系统日志分析结果而言，海莲花组织的恶意指令都是从服务端发出的，这说明他们可能没有利用这个漏洞，或者还存在其他攻击手法。”佳佳表达了自己的怀疑，并且这个怀疑很快得到了大家的认可。

顿时，众人陷入了沉思。

一番思索之后，佳佳很快将怀疑目标放在了补安软件服务端的登录凭证上。如果海莲花组织是通过已经泄露的凭证登录的，那么服务端登录日志一定有异常。果不其然，从 2020 年 7 月上旬开始，服务端已经出现过多次异地登录，并且时间线和海莲花组织入侵时间非常吻合（2020 年 7 月中旬，NGSOC 首次记录海莲花组织此轮 APT 攻击告警）。

“那口令到底是怎么泄露的呢？能查出来么？”水子哥连忙问到。

“这不好说，很难查。”佳佳叹了一口气，口令泄露的方法有太多太多种，有可能是撞库攻击，有可能是你们登录口令没有经过加密存储，也有可能是谁上传到 GitHub 上了……”

“但眼下最重要也是最紧急的任务是，为了保险起见，尽快把集团内部重要的登录口令全部更换一遍，并且制定定期更换的规则。另外，安全软件自身的漏洞更要重视，需及时安装补丁。”佳佳说。

安全软件从来不是绝对安全的，它和比普通软件一样，也可能存在各种各样的漏洞和口令泄露的风险。并且，由于安全软件相对普通应用软件而言，系统权限较高，一旦被黑客利用危害也更大。因此，安全软件也需要安全运营工程师的常态化运营，才能最大化发挥出网络安全的效果。

——后记 安

四个转变 看能源巨头 国家电投的网络安全运营之路

“你只有探索，才能知道答案。”
——法国作家儒勒·凡尔纳

作者 奇安信公关部 张少波
奇安信 NGSOC 产品咨询专家 张华

“在网络安全运营这条道路上，国内几乎没有能借鉴的行业成熟先例，没有可参考的成功经验模式，只有通过自己的探索，才能找到适合集团自身的运营模式。”国家电投集团信息技术有限公司网络安全部副总经理（国家电投集团网络信息安全实验室副主任）张萌多次提及“探索”这个词语，概括了这家清洁能源巨头在安全运营实践中的心路历程。

作为我国五大发电集团之一，国家电投集团（全称为国家电力投资集团有限公司），是中央直接管理的特大型国有重要骨干企业，肩负保障国家能源安全的重大责任，致力于建设具有全球竞争力的世界一流清洁能源企业。2020 年，国家电投在世界 500 强企业中位列 316 位，业务范围覆盖 46 个国家和地区，现有员工总数 13 万人，拥有 62 家二级单位，其中 5 家 A 股上市公司、1 家香港红筹股公司和 2 家新三板挂牌交易公司。

在信息化和网络安全方面，国家电投一直按照价值导向、问题导向砥砺前行。早在 2016 年，当网络安全防护建设仍处于设备堆砌阶段之时，国家电投就已意识到运营的紧迫性和必要性，并率先开启了安全运营探索之路。

从产品堆叠到运营为先

2015 到 2016 年，网络安全行业正在经历一场历史性的变革，以数据驱动为核心的安全理念，正式登上了历史舞台。适逢 RSAC 2016 提出“connect to protect（用连接去保护）”，以被动防御为核心、机械堆叠网络安全设备的方式逐渐走向了历史。

“在 2016 年以前，整个行业都普遍存在一个状况，虽然部署了很多网络安全设备，却无法回答集团领导的三个灵魂拷问：谁攻进来过？干过什么？什么东西被拿走了？即便是到现在，也有大量的机构不能回答这三个问题。” 回想当年的行业网络安全现状，张萌依然是记忆深刻。

“那些年，大家对网络安全建设都是以购买安全产品为主，没有安全运营的概念，大家基本上就是按照当时的等保合规等监管要求，安装防火墙、杀毒软件、入侵检测系统这些，再安排几个人，保证这些设备正常运转就可以了。”

然而在信息化建设和数字化转型不断深入，新型网络威胁尤其是 APT 攻击、勒索病毒等层出不穷的背景下，电力行业作为关键信息基础设施，其网络安全重要性日益凸显。越来越多企业意识到，即便堆砌再多的网络安全设备，也无法改变“盲守”、被动挨打的情况，建立更积极主动的安全防护体系势在必行。

“和很多单位不同的是，从一开始，我们的理念就是以运营为核心，而不是仅仅按照合规的要求，部署相应的产品、平台或者工具。”张萌表示。

在运营为先的思想指导下，2016 年开始，国家电投逐步建立了覆盖全集团大部分单位的 SIEM（安全信息和事件管理）平台，以大数据作为底层架构，采集全量系统日志，实现安全事件的监控和应急处理。

然而，安全团队很快发现，SIEM 想要充分发挥自身的价值有着很大的局限性：作为彼时最炙手可热的安全产品和技术之一，SIEM 需要依赖高质量的日志，从中找出潜在的非法行为。很快一个难题就出现了，也就是日志采集。日志采集绝非“眉毛胡子一把抓”的过程，这其中涉及到日志的类型、内容、存储、检索、分析，以及跨部门的协调、管理等等诸多挑战，都需要安全团队一一解决。

“在当时的情况下，这些问题都很棘手。”张萌表示，“不能否认 SIEM 是好产品，但缺乏有效的安全运营手段。就像一个厨师，应当按着自己心中的菜谱搭配食材，而不是对着杂乱无章的厨房，构思着虚无缥缈的满汉全席。”

从合规驱动到实战导向

到 2019 年，国家电投在思路上有了显著的变化。那一年，公安部提出了“三化六防”新思想，以“实战化，体系化，常态化”为新理念，以“动态防御，主动防御，纵深防御，精准防护，整体防护，联防联控”为新举措，构建国家网络安全综合防控系统，深入推进等级保护和关键信息基础设施保护的积极实践。在网络安全防护体系建设中，国家电投不仅单纯考虑政策监管和合规需求，更要将 “三化六防”理念贯穿进去，其中率先落地的就是实战化和常态化。

“基于实战化的思想和需求，我们第一步要解决威胁检测的问题。比如我们拥有什么资产？这些资产有哪些脆弱点？是否被攻击？具体是什么攻击？攻击是否成功？攻击的影响是什么？该采取什么应对措施？应对措施是否有效？未被攻击的如何预防？这其实就是国家电投现在所说的安全运营要完成的工作。”

张萌认为，区别于过去面向合规的安全运维，安全运营更强调网络安全与信息化的融合，通过运营过程，让网络安全人员与设备发挥出应有的效果，从而实现网络安全风险可控可接受的目标。

在这一年，国家电投部署了奇安信态势感知与安全运营平台（NGSOC），以 NGSOC 作为安全运营工作的核心威胁感知支撑工具，在实战化安全运营方面迈出了重要一步。

“实战化安全运营体系的建设不是一蹴而就的，我们上线 NGSOC，首先要解决谁来攻击，用什么方式的

图：国家电投综合安全态势大屏

问题，让安全威胁可见、可知、可控。否则就是两眼一抹黑，看不到敌人、被动挨打。”

NGSOC 上线的效果也是立竿见影。安全运营团队借助奇安信 NGSOC 平台的技术支撑能力，同期构建无缝协同联动机制，国家电投在安全监测预警、威胁分析和主动防御方面的能力大幅提升。自上线来，月均采集和存储约 89 亿条安全日志，月均发现约 75 起威胁攻击，包括 webshell 上传、挖矿木马、勒索软件、远控木马等破坏性强、影响范围大的高威胁安全事件。

在资产梳理及漏洞修复方面，NGSOC 上线至今，持续梳理总部资产及下级单位资产、网段信息，对多个系统进行漏洞检测、修复及复测，修复率高达 91%。

而在 2020 年网络攻防实战演习中，运营团队通过 NGSOC 对威胁告警进行监测分析，发现并处置安全威胁事件 65 件，结合威胁情报信息共封禁攻击 IP 地址 74667 个，提交防守报告 16 份，圆满完成了防守任务。

从局部实践到规模化推广

当国家电投通过集团数据中心以及数家二级单位，完成探索成功的第一步之后，下一步的任务，就是按照集团公司统筹规划，将该模式推广到整个集团。

据介绍，目前安全运营中心主要覆盖了数家单位，包括集团数据中心、中国电力、成套公司、山东核电、姚孟电厂、横琴热电、重燃公司等等。按照集团规划，2021 年，计划在集团范围全面扩展覆盖，堪称近百倍级的量级扩张。

“量变势必带来质变，随着未来集团安全运营中心的建立，将面临效果和效率的双重挑战。”张萌表示。

首先是效率方面的挑战。目前，网络安全运营在集团数据中心已经稳定，每天产生 2 亿多条日志，告警归并之后，大约 2000 多条告警。这些告警主要依赖于专业人员来分析处理，效率比较低。在规模化后，预估日均告警数量将有数十倍甚至百倍的提升，投入数十倍的员工当然是不现实的，因此必须提升安全运营的效率。例如整合 NGSOC 平台和主机安全系统，实现安全威胁告警自动化分析判断；再例如面对历史同类的告警，系统按照现有的 SOP 执行自动化的分析判断。

“在这个问题上，我们也在测试最近比较火热的 SOAR 产品。从技术理念上来说，我们将所有的安全产品划分为三个阶段使用，‘感知’阶段、‘分析与辅助决策’阶段、‘行动’阶段。SOAR 能提供自动化安全编排和响应能力，我们将 SOAR 定位为‘分析与辅助决策’阶段和‘行动’阶段的‘执行管家’，希望能在规模化运营时期，大幅度提升我们安全运营的分析与行动效率。”

第二是来自效果的挑战。随着规模越来越大，网络环境越来越复杂，威胁数量、攻击形式都会激烈增加，

安全运营需要对威胁预警和脆弱性，实现更全面、更精准的发现和处理。

如何解决这些问题，国家电投已探索了很多经验。举例来说，在日常和实战攻防演习期间，国家电投优先修补有公开 POC 或者 EXP 的漏洞（即已验证可被利用的漏洞），而不是追求大而全、修补所有漏洞，这样能在投入（工作量）和安全风险之间寻求相对平衡，在尽量降低安全风险的同时，又符合安全运营的投入产出比原则。

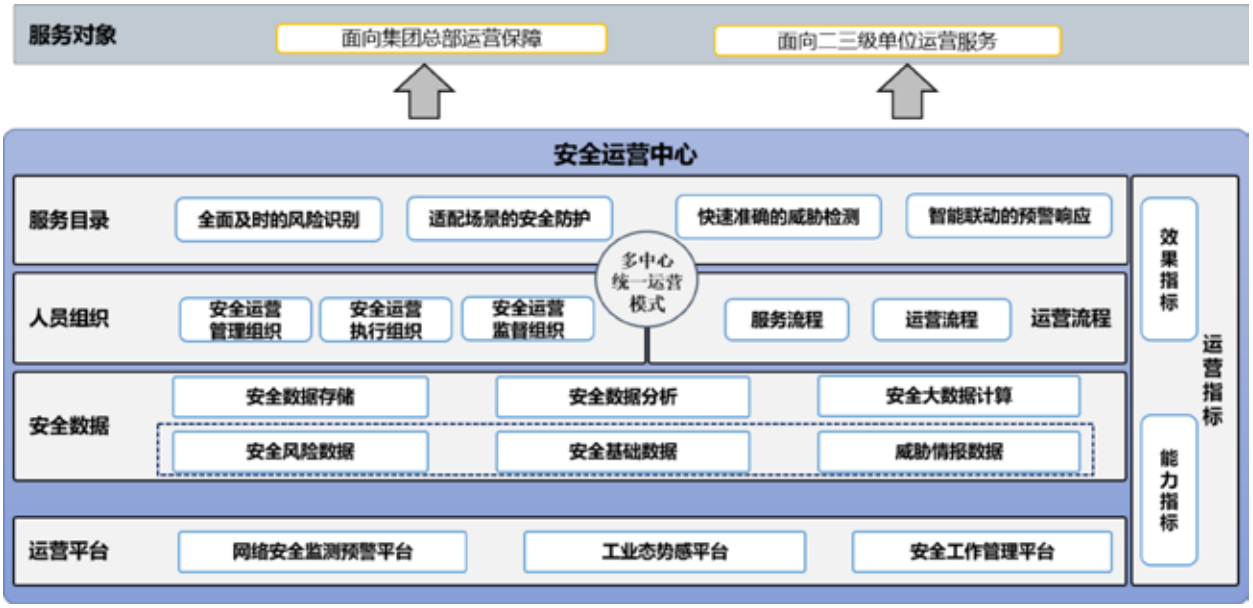
同时，国家电投非常注重场景积累和经验复用。张萌表示，没有绝对的网络安全，将所有未知的威胁全部阻断是非常不现实的，因此我们的重点目标，是避免系统被相同的攻击手法打穿两次，不能在一个问题上反复栽跟头。所以遇到一类问题，一类场景，都将其沉淀下来，形成标准化的 SOP 积累，为将来全面走向系统化提供基础。

截至目前，国家电投安全运营团队总结出了 12 类大场景，若干个小场景，并将其运营工作固化下来，以便能够让新的安全运营人员快速上手复用，满足规模增长和人数增长的需求。同时为系统功能更新、SOAR 自动化编排等做准备，实现自动化编排，显著提升效率。

从能力输出到价值共鸣

“沿着旧地图，找不到新大陆”。探索的道路注定布满荆棘，在网络安全运营这条路上，有国内领先安全企业的持续参与，国家电投走的并不孤独。张萌表示，“我们选择合作伙伴，不单考虑对方的产品和技术能力，更要考虑双方是否有共同的运营价值观和运营理念。”

展望“十四五”期间，张萌提到，国家电投将继续坚持高标准要求、高目标定位、高水准建设理念，在“十三五”基础上，构建一体化的安全管控体系、安全技防体系、安全运行体系，全面实现“由被动防护转向主动防御、由静态保护转向动态保障、由加固监测转向安全可控”的三个转变，打造“精细化安全管控、体系化主动防御、实战化安全运行”的总体效果，为集团公司建设具有全球竞争力的世界一流清洁能源企业，提供强有力的支撑保障。 安



图：国家电投安全运营框架图

商业银行零信任安全架构研究

作者 上海浦东发展银行信息科技部
崔兆栋 田益 王京峰

云计算、大数据、移动互联网等新技术的发展，催生出移动办公、业务上云、外部生态对接等新场景，也带来商业银行 IT 技术架构的变革。传统安全架构以边界为中心进行安全防护，为解决新场景提出的数据开放和共享问题，需开启更多的边界策略，导致管理复杂度增加，同时带来新的安全问题。在这种背景下，不再仅依赖网络位置，而是通过持续度量身份来动态构筑安全边界的零信任安全架构理念脱颖而出。

为了更好地构建企业 IT 安全防护体系，有效支撑数字化生态银行战略目标，上海浦东发展银行（以下简称“浦发银行”）参考国际及国内零信任架构理论和实践，开展了零信任安全新架构课题研究，从理论模型、规划设计、实践验证的角度全面研究了零信任架构的可行性。

一、研究背景

近年来，随着科技的不断创新与发展，企业业务、数据与外部的深入交互使网络边界逐渐模糊，仅依赖网络层策略难以解决数据泄露等安全风险。外部攻击和内部威胁是造成企业数据泄露的两大主因。

外部攻击的一般途径是通过社会工程学对目标人员实施攻击并获得初始控制权，然后通过在目标网络横向平移或 PowerShell 后门的方式完成攻击；

内部威胁往往是因为企业员工或运维人员拥有特定业务和数据的合法访问权限，一旦出现凭证丢失、权限滥用或非授权访问等问题，会导致企业数据的泄漏。仅通过开启防火墙、入侵防御系统等方式无法解决内部威胁问题。

传统的网络安全架构围绕网络边界布防，假设或默认了内网比外网更安全，在某种程度上预设了对内网中的人、设备和系统的信任。攻击者一旦突破网络安全边界进入内网，默认信任极有可能成为攻击者手中的有力武器。

零信任的本质是在访问主体和客体之间构建以身份为基石的动态可信访问控制体系，围绕着以身份为基石、业务安全访问、持续信任评估和动态访问控制四大关键能力，对默认不可信的访问主体的所有访问请求进行加密、认证和强制授权，基于各种数据源进行持续信任评估，最终在访问主体和访问客体之间建立一种动态信任关系，并根据信任的程度授予访问权限。

二、研究目标

零信任安全新架构课题研究目标包括以下三个。

目标一：零信任架构通用理论模型研究

高度提炼总结业务场景中的关键因素，形成具备普适性的零信任架构通用理论模型，用于指导企业在面临多种业务场景（日常办公、移动办公、开放银行等）、多方人员（正式员工、外包人员、外部生态等）、多类设备（PC 设备、移动设备等）情况下，能够结合现状及需求完成规划方案设计。

目标二：商业银行典型场景零信任安全规划设计

针对办公场景、移动办公、开放银行三个典型场景，规划设计商业银行零信任安全规划设计方案。

办公及移动场景：依据构建的零信任理论模型，结合商业银行已具备的安全能力，通过构建用户行为分析、终端安全感知度量、多源数据联合分析、访问策略动态调整等能力，形成零信任规划方案。

开放银行场景：开放银行场景在用户身份验证、接口权限的有效控制、防止未授权访问、动态调整权限、缩小暴露面、第三方安全状态等方面都面临新的安全挑战。零信任架构理念契合开放银行对于安全的需求，需要规划设计开放银行零信任方案。

目标三：办公场景零信任 POC(Proof of Concept) 测试验证

基于办公场景进行 POC 测试验证，设计 POC 测试方案，搭建测试环境，通过丰富的测试用例验证零信任架构在办公场景下的效果，验证零信任架构的可行性。

三、研究内容

1. 零信任架构通用理论模型

零信任架构通用理论模型抽象出主体、客体、数据流三要素（如图 1 所示），建立主客体间的访问规则，确保数据流的安全可控。其中，主客体间的数据流规则基于主体信任等级与客体安全等级的匹配规则实现，采用资产安全等级、用户信任等级、设备信任等级、动态授权模型、业务安全访问模型描述。

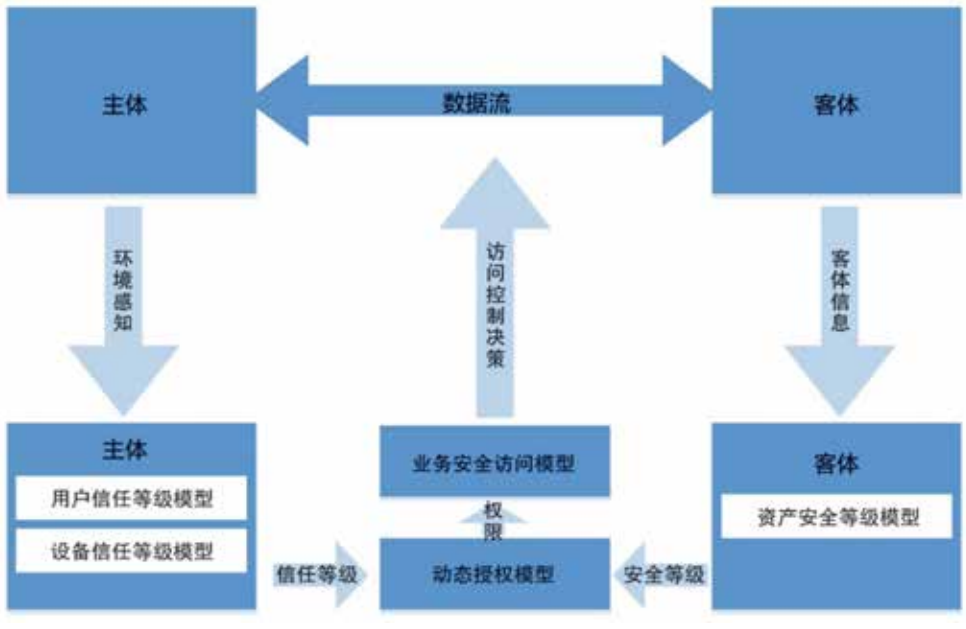


图 1 零信任架构通用理论模型

(1) 资产安全等级模型

用于定义资产安全等级的划分方式——分阶段、由粗到细。第一阶段，粗粒度划分，按照应用系统包含数据敏感程度、数据重要性等维度划分为“公开、内部、秘密”三级。第二阶段，细粒度划分，与企业资产特性及安全需求密切相关。逐级安全

等级划分方式可更好地适应企业差异性。

(2) 用户信任等级模型

用于评估用户可信度，通过对用户行为的推理分析实现。推理分析通过一系列模型实现，不同分析模型权重不同，利用模型对用户行为评分并映射到对应的用户信任等级。企业根据能够采集到的数据类型、业务安全需求选择合适的模型、调整权重，评估用户信任等级。

(3) 设备信任等级模型

用于评估设备可信度，通过合规基线规则实现。合规基线规则从设备、系统、软件、网络、环境等多维度来评估设备信任等级，可按照企业安全需求进行设计。不同信任等级合规基线规则不同。

(4) 动态授权模型

用于规范主体到客体可访问的内容及操作，只允许授权通过的主体访问客体。动态授权模型结合基于角色的访问控制、基于属性的访问控制和分级访问控制设计实现，支持细粒度授权及基于风险的动态权限调整。当主体信任等级等于或高于访问资产所需的最低信任等级时才授予访问权限，并根据主体的持续评估结果动态调整权限分配。

(5) 业务安全访问模型

用于保证主体对客体业务访问过程的安全可控，通过认证机制、访问控制策略、业务安全策略、通道加密四大安全措施实现。认证机制提供用户、设备的身份认证；访问控制策略由动态授权和信任评估的结果共同决定，基于动态访问控制策略执行主体对客体的访问控制；业务安全策略包括业务隐藏、流量控制等；通道加密是确保主客体之间数据的安全传输，通常基于标准 TLS 安全隧道实现。

2. 安全认证规划设计

安全认证规划设计方案涵盖办公场景、移动场景、开放银行场景三个方面，零信任规划全景如图 2 所示。

(1) 办公场景零信任规划设计

办公场景零信任规划方案的设计可充分结合商业银行现已具备的安全能力，如身份及权限服务、终端管控、态势感知等第三方监测平台，结合零信任组件构建以身份为基石、业务安全访问、持续信任评估、动态访问控制核心的安全能力。

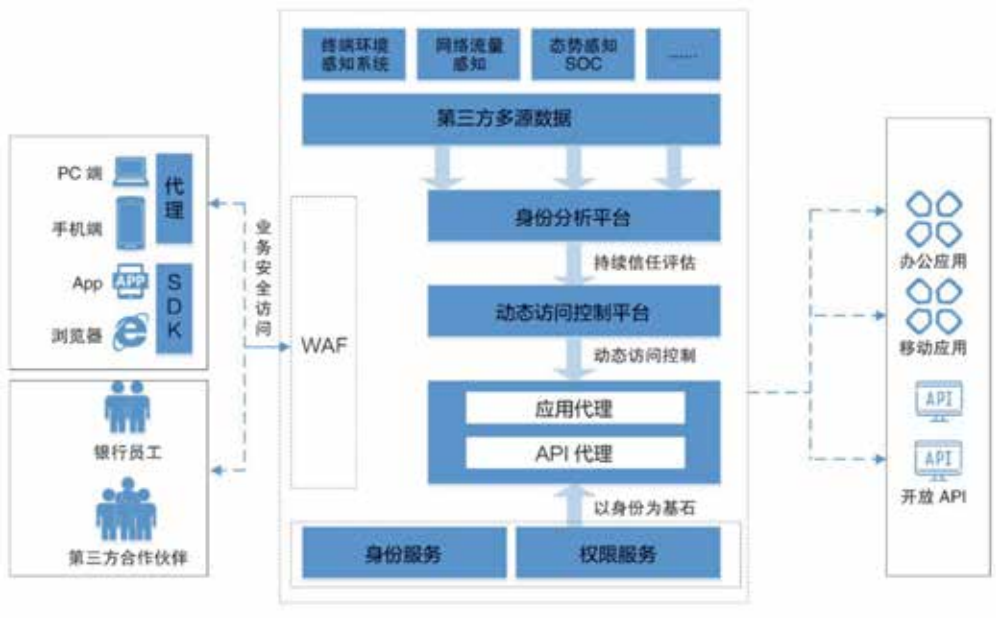


图 2 零信任规划全景展示

零信任组件包括终端环境感知代理、终端环境感知系统、身份分析平台、动态访问控制平台、应用代理。

· 终端环境感知代理感知设备环境风险，将终端风险状态及设备信息等上报至终端环境感知系统。

· 身份分析平台是动态访问控制的分析引擎，基于终端环境感知系统上报的终端环境感知、用户访

问日志及第三方监测平台上报的日志及事件信息，对终端环境和用户行为进行风险分析，实现持续的信任评估，并将评估结果推送至动态访问控制平台。

· 动态访问控制平台是访问控制的策略判定点，能够接入或提供身份及权限服务，提供自适应多因子认证能力；同时接收身份分析平台持续推送的信任评估结果，为应用代理提供动态授权判定，及时阻断存在风险的会话或进行二次认证。

· 应用代理是策略执行点，通过代理技术实现业务安全访问，根据动态访问控制平台下发的策略提供应用级细粒度访问控制。

(2) 移动场景规划设计

移动场景零信任规划方案的设计可充分结合商业银行现已具备的安全能力、移动安全防护手段等，通过零信任组件构建移动场景零信任安全架构核心安全能力。

零信任组件包括移动终端环境感知代理 (Agent 或 SDK)、安全接入 SDK、移动终端环境感知系统、身份分析平台、动态访问控制平台、应用代理。其中移动可信环境感知代理感知 BYOD 设备环境风险，包括风险评估、应用合规信息等设备安全状态，并将信息上报至移动终端环境感知系统；安全接入 SDK 与应用代理建立安全通道；身份分析平台可基于移动终端环境感知系统上报的环境感知信息进行风险分析，实现持续信任评估，并将评估结果推送至动态访问控制平台；动态访问控制平台是访问控制的策略判定点，能够接入或提供身份及权限服务，提供自适应多因子认证能力；同时接收身份分析平台持续推送的信任评估结果，为应用代理提供动态授权判定，及时阻断会话或进行二次认证；应用代理是策略执行点，根据动态访问控制平台下发的策略提供应用级细粒度访问控制。

(3) 开放银行场景规划设计

商业银行通过 API 直接连接或 SDK 间接连接的方式向应用方和用户提供 API 服务。相较传统银行，开放银行带来了一系列安全风险。《OWASP TOP 10》报告中指出，身份认证不足、数据过度暴露、缺乏资源和速率控制、授权粒度太粗、错误的安全配置、注入攻击、不足的日志和监控等问题是导致 API 安全问题的重要因素，在进行 API 安全防护体系设计时，应考虑端点的安全性 (如 SDK)，API 接入的访问控制 (包括终端用户 / 应用的身份认证、API 接口及资源对象的细粒度授权管理、通道加密、流量控制等) 以及安全分析与防护能力，提供对于 API 接口调用的动态访问控制能力，在分析检测到 API 调用风险时能够及时阻断或调整权限。

开放银行场景零信任规划方案可充分结合商业银行现已具备的安全能力，融合身份与权限服务、API 代理、身份分析平台、动态访问控制平台、终端环境感知 SDK 能力构建。

· 由身份与权限服务提供身份管理、身份认证与权限的管理等能力，包括用户令牌、访问令牌发放与验证；

· 由 API 代理提供业务安全访问能力，包括通道加密、流量限制、协议内容解析、令牌转换等功能；

· 由身份分析平台提供基于身份的监测和分析的能力，由动态访问控制平台提供动态访问控制能力，在监测到 API 调用风险时下发策略进行阻断或调整权限；

· 由终端环境感知 SDK 提供终端环境数据采集。

3. 办公场景零信任 POC 测试验证

办公场景零信任 POC 测试选择在开发测试环境进行验证，用户通过云桌面方式访问测试应用。方案遵循对现有网络及应用影响最小的原则设计，前期准备工作包括：机房部署应用代理、动态访问控制平台、身份分析平台、终端环境感知系统四台设备；办公 PC 测试机安装终端环境感知 Agent；动态访问控制平台、身份分析平台、终端环境感知系统、身份及权限系统对接；配置测试应用；用户访问和动态访问控制流程调试。办公场景零信任 POC 流程如图 3 所示。

其中，动态访问控制的逻辑流程为：

(1) 终端环境感知 Agent 实时感知终端环境安全风险并上报至终端环境感知系统；

(2) 终端环境感知系统将感知结果上报给身份分析平台；

(3) 身份分析平台结合感知结果及应用代理、动态访

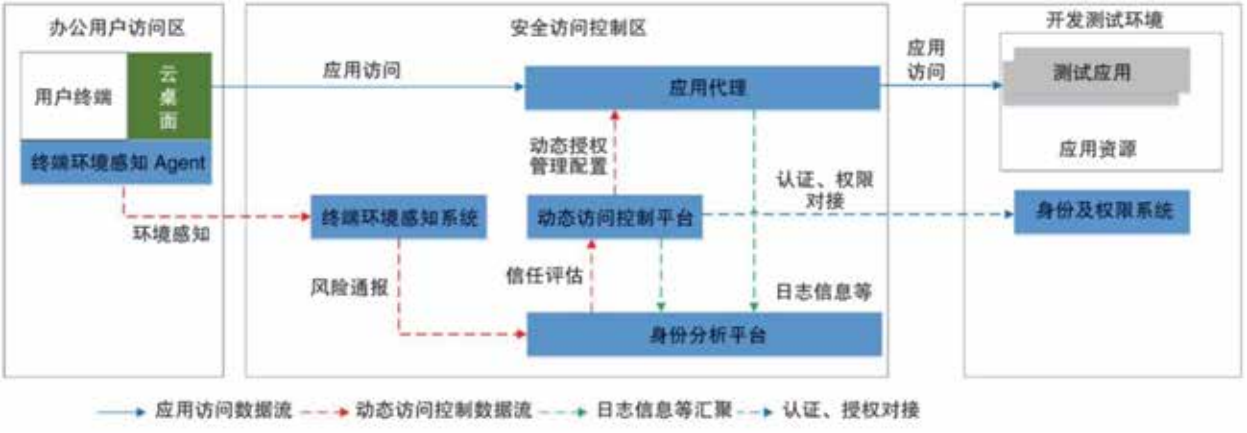


图 3 办公场景零信任 POC 流程

问控制平台的访问日志，完成终端设备安全状态及用户行为分析，将最终的分析结果上报给动态访问控制平台；

(4) 动态访问控制平台根据身份分析平台的分析结果，判断当前方式是授权访问还是阻断，最终达到动态访问控制效果。

基于测试环境具备条件，POC 从终端可信环境感知、基于属性的动态访问控制、用户行为分析三大能力点，初步通过共计 12 个测试用例的验证，输出零信任办公场景测试报告 (见表 1)。验证表明，办公场景零信任方案具备在实际应用环境中的可落地性与有效性，可实现商业银行办公场景的零信任动态访问控制，满足行内对内部应用系统安全访问控制的功能规划。

四、总结及展望

本文通过对零信任安全架构进行深入研究，在理论研究、规划设计、落地实践三个方面都取得了相应成果。在理论研究方面，形成了具有指导意义的通用理论模型；在规划设计方面，完成了办公场景、移动场景、开放银行场景三种商业银行典型场景的零信任安全规划方案；在落地实践方面，在真实的开发测试环境通过 POC 测试验证了方案的可行性。课题成果为后续浦发银行开展零信任架构建设奠定了基础，同时也为商业银行开展网络和应用安全建设提供了一定参考。零信任架构的实践还需考虑逐步迁移问题，未来浦发银行会结合实际场景下问题逐步完备方案，解决业务迁移、C/S 业务零信任等实际问题。安

能力点	测试用例	测试结果
终端可信环境感知	终端受控设备管理	通过
	可信环境评分	通过
	应用合规感知 - 黑名单软件监测	通过
基于属性的动态访问控制	基于可信分的动态访问控制	通过
	基于 IP 的动态访问控制	通过
	基于时间的动态访问控制	通过
	基于浏览器类型和版本的动态访问控制	通过
	不同用户的动态访问控制	通过
用户行为分析	基于时间的用户行为分析	通过
	基于访问频次行为的用户行为分析	通过
	基于常用设备的用户行为分析	通过
	基于账户冒用的用户行为分析	通过

表 1 零信任办公场景测试报告

奇安信
新一代网络安全领军者

云安全管理平台

云安全的智慧大脑

运用软件定义安全的设计思路，将云的属性赋能给安全体系

在公共服务云安全建设中，协助云服务商搭建可按需交付、分权管理和业务增值的云安全资源池。在行业私有云安全建设中，使安全具备敏捷上线、集约化部署和易于统一监管的能力。云安全管理平台为各行业客户提供安全产品服务化、安全能力一体化、安全运营自动化 三大核心价值，为云保驾护航。

从程序媛到事业部领头人
常月姐姐的“乘风破浪”

作者 公关部 孙丽芳

“不要发邮件了，这个事情咱们马上和前方拉个视频会，今天必须解决！”一片焦灼的讨论声中，一句清脆的女声一锤定音。

众所周知，网络安全行业是一个技术硬核行业，因此 IT 男扎堆儿，阳刚气十足。而奇安信态势感知第一事业部的领头人，按照时下的说法，却是一位乘风破浪的姐姐。名字娴静温婉，“梨花院落溶溶月，常在人间四月天”。

从 2016 到 2020 年，随着《网络安全法》和《国家网络安全战略》的相继出台，态势感知成为网络空间安全领域聚焦的热点。而多家第三方机构的市场分析报告显示，奇安信在态势感知领域始终处于领先地位。

要了解这一切，有一条捷径，那就是走近这位名叫常月的姐姐。

火线支援 一战成名

2011 年 3 月，常月入职成为网神 SOC 技术团队一员，从基层程序媛干起，逐步成长为了技术骨干。2015 年，常月随团队一起，并入奇安信。之后虽然一直稳打稳扎，从研发经理又成长为技术团队 Leader，但在人才济济的奇安信，常月并不惹眼。

直到 2018 年，常月“一战成名”。

2017 年 12 月，公司在某大型央企客户的项目出现了问题。客户表示，如果问题不能解决，将让奇安信的产品全面退出其市场，且几年内都不能再进入。丢掉一个大型客户，损失一大块市场，这是公司绝不允许的。公司董事长齐向东要求项目组立刻全面整改。这次出现问题的是设备，也直接反映在了设备集中管理软件中，出现了丢策略和下错策略的情况。

面对如此棘手的问题，项目组有些束手无策。

当务之急，从公司内部找高手！

曾担任过 SOC 研发团队 Leader 的常月成为第一人选。

“有点懵，2015 年我就不在 SOC 了，这个项目完全没有参与过。项目现在也有技术负责人，我一个人从外面突然进入，技术上、人员上的头绪都很难理清。我怕自己把事给耽误了”。最开始，常月也有些顾虑。

“但是客户的需求是第一位的，我自己的困难自己

图：2016 年常月和当时的团队小伙伴

解决，先把活儿干了”。常月一头扎进了项目，快速与团队建立信任，了解情况，诊断问题，明确优化方案，不分晨昏连续加班，10 天后，交出了一版方案，技术人员根据方案进行迭代，解决了第一波危机。

2018 年元旦当天，常月接到齐总的电话，要求速回公司开会，项目又出现了新的问题。放下电话，常月马上赶到了公司。这一次，常月带领临时团队（由 3 个产线成员组成）封闭驻项目 20 多天，抽丝剥茧，又拿出了一版方案。经过压力测试，在保持用户数正常增长的规律下，半年内不会再出现问题。常月平稳地把接力棒交回给了 SOC 研发团队。项目后续运行平稳，客户满意度很高。常月正式退出项目组。

临危受命不但没有耽误事，还把事漂亮地解决，常月在公司内部开始为人所熟知。齐总亲自号召大家向她学习。

“这次算是对其他产品的火线支援，可能干得还行，大家对我的肯定是一种鼓励。但当时我更想的，是怎么能在自己负责的产线做出一番成绩，我觉得它的潜力很大。”

成就客户 成就彼此

这条让常月想大干一番的产线，就是公司的态势感知产品线（安全监管 BG 的前身）。

态势感知的概念最早在军事领域被提出，随着网络安全重要性的凸显，开始在网安领域展露头角。从技术思潮到成型产品到被市场广泛认可，奇安信态势感知一直位于前列，对行业发展起到了引领作用。

而事实上，奇安信态势感知最初也走过艰难的探索阶段。

“我们的第一个项目是青岛网安态势感知，当时核心是为了保障 2018 年在青岛举行的上合峰会。从 2016 年开始，我们就提前投入进行支持。但当时态势感知还只是一个概念，具体怎么做，双方都不清楚，没有先例。所以早期基本是客户带着我们做。”

这样的状态显然非常被动。

“客户说啥就干啥，我们以为是做到了客户优先，但效果并不好，团队疲于奔命，但客户并不满意”。

尽管如此，时任态势感知研发总监的常月没有气馁，带着团队和客户不断碰撞，摸索着解决方案。“这块硬骨头一定要啃下来，不能辜负客户信任，也是为奇安信态势感知正名”。

2018 年上半年，青岛的上合峰会筹备工作进入冲刺阶段。

而此前在客户身后亦步亦趋的奇安信态势感知，也逐渐找到了感觉。

“我们开始深入挖掘客户需求，站在客户的立场想问题”。常月带队驻场青岛两个多月，全月无休，一点一点将平台最终搭建完成。平台除了能满足客户提出的要求，很多方面甚至想在了客户前面。

万事俱备，只待峰会开幕，奇安信态势感知一显身手。

然而就在峰会开幕的前一晚 10 点，奇安信团队接到客户的突发需求。

原定于次日上午 10 点，由奇安信向公安部领导汇报峰会重保和平台建设情况，改由青岛网安进行汇报。一个是厂商视角，一个是客户视角，汇报的方式区别很大。客户对此没有准备。唯一的方法就是奇安信迅速调整出一套适合客户汇报和演示的方案。客户要求，次日早 8 点，方案调整到位。

常月作为值守代表正在现场。“明天就开幕了，不能打乱部署，其他人不能动了。项目的情况、客户的思路我清楚，我来”。常月主动接下了任务。

原本的汇报方案全部打乱，牵一发而动全身。常月通宵达旦，找关键素材，验证数据，向客户确认，重拟方案。

次日早 8 点，常月准时走进客户办公室，和客户对调整后的汇报方案进行最后的交流。

上午 10 点，客户圆满完成了现场汇报。因为数据充足、逻辑清晰、效果明显，公安部领导对青岛网安的重保部署及奇安信网络安全协调指挥平台给予了高度评价。在随后开幕的上合峰会上，奇安信不辱使命，圆满完成了保障任务。

而与此同时，团队再次接到客户的突发需求。

峰会闭幕后，全国网安系统要在宁波召开现场会，根据此前的汇报情况，公安部领导下达指示，重点由青岛网安现场进行态势感知项目建设的分享。这次的汇报材料仍由奇安信进行支持，材料要更加细致，准备时间共三天。

常月二话没说，再次亲自准备。她每半天和客户碰一次，撰写了 200 多页 PPT，最后又精炼为 50 多页。

最终，客户的分享效果非常好，专门向奇安信表达了感谢。作为业内先行者，青岛网安态势感知项目在会议现场引起强烈反响。而在客户 30 分钟的汇报时间里，至少点名表扬了奇安信 10 多次。

“通过态势平台高质量保障上合峰会的成效，让我们感觉到与客户走近了。这两次汇报的事，也很有意义，我们满足了客户的突发需求，成就了客户，客户也更加接纳我们”。

而在随后，常月带领团队，进一步挖掘到了客户的深层次需求，利用态势感知 S 版平台帮助客户挖掘案件线索，并配合破案，真正成就了客户，真正做到了客户优先，也赢得了客户的高度认可。客户甚至主动为奇安信宣传。

青岛网安标杆项目的意义很快显现，在青岛之后，天津、贵阳等地的网信、公安、工信等监管机构、各级政府部门纷纷启动了监管类网络安全态势感知平台的建设。奇安信态势感知大显身手。而在众多国家级重大活动网络安全保障中，奇安信态势感知一直承担了指挥平台的重要角色。

落好关键子 下活一盘棋

态势感知市场逐步成熟，2019 年，在集团副总裁李虎的推荐下，常月升任态势感知事业部总经理。

从研发管理到全面管理，常月的工作更加忙碌。频繁出差，对重点项目、标杆项目进行支撑，带领团队“攻城拔寨”，也成为常月工作的常态。

虽然“身经百战”，但 2020 年的一场“战役”，让常月记忆犹新。

某省在互联网普及率、政府数字化转型、网络综合治理等领域都走在全国前列。然而就是在这样一个网络大省、网络强省，奇安信态势感知多年来颗粒无收。

“原因有很多，其中很重要的一个就是某友商的大本营就在该省，深耕该省网络安全市场多年。就像一盘棋，长期以来，我们一个子都落不下。”常月心里一直憋着一口气。

破局的机会终于在 2020 年到来。

2 月，该省网络安全与协调指挥平台启动三期项目的招标。

“2017-2020 年，该友商是该省平台建设的核心厂商。但平台建成后，实际成效尚未能达到客户预期的效果。三期项目希望加强安全能力，对现有数据二次分析，以提升实战成效。”该省分区的销售第一时间把项目现状、机会点在公司内部进行了汇报。

虎口夺粮，实现该省态势感知市场零突破，项目的战略意义不言而喻。公司领导高度重视，要求产线全力支持，工作实施主要由常月负责。

态势感知事业部的研发中心设在北京和武汉。而当时正是新冠疫情最肆虐的时期。武汉已经全民居家，北京的疫情形式也非常紧张。常月带领团队先是远程和区域销售一起讨论，出方案、出策略。疫情稍缓解，常月

图：支撑浙江网信项目的奇安信态势感知团队

灵活调配两地研发人员，轮流去客户现场支撑，自己则频繁前往。

策略得当、前后端配合无间， 7 月 3 日，奇安信中标该省三期平台。“这个项目的金额并不高，但是对态势感知产线，对公司，意义都非常重大，该省这盘大棋我们终于撕开了一个口子，落下了一子！” 对于来之不易的胜利，常月难掩兴奋。

但无暇庆功，常月和团队很快面临新的挑战。

9 月 28 日产品从北京发货，客户要求十一之后就要交付，并且要看到运行效果。这意味着安装调试必须从十一假期开始，而且在初期接入数据，数据量有限的情况下，要产生较好的效果就必须拟制针对性的运行方案。

“销售已经敲开了门，能不能守住阵地，并发扬光大，后面要看我们的了”。常月一边安排人手火速前往支持调试，一边牵头研究拟制运行方案。

10 月，在区域销售、现场项目经理、常月团队的共同努力下，项目如期顺利交付。

在本项目中，奇安信部署了 2 台流量探针，某友商部署了远多于奇安信的流量探针并独家掌握了全省网站云监测数据，在此前提下，奇安信做到了客户认可的高价值安全事件发现量在所有厂商中名列第一。

“客户的需求很明确，希望提升网络安全威胁深度发现能力。我们在项目第三期才进入，数据条件远不及友商，所以我们要充分发挥自身安全能力的价值。我们综合安全分析人员、驻场安全运营人员、威胁情报、流量探针、态势感知，做了一套相对完善的方案。用通用的方式可能达不到这么好的效果，针对我们的客户，特定的网络环境，我们调整打法，对安全分析视角进行了全面优化。”

数据最有说服力，客户对奇安信设备运行效果非常满意。奇安信态势感知也因为这关键一子，盘活了该省市场的整盘棋。继该省级平台之后，该省若干地市陆续上线了奇安信态势感知产品。产线在该省大数据局、多个地市大数据局也有了产出。

“天时不如地利，地利不如人和。我们在第三期才挤进竞争极度激烈的友商根据地市场，能赢得客户的认可，后来者居上，很大程度上是因为我们对客户优先理解的不断加强。我们作为一个专业公司，要能够发挥专家作用，真正站在客户角度，帮助客户谋划、帮助客户成功。只要真正做出了成效，就会得到客户真心认可，从而实现共赢。”

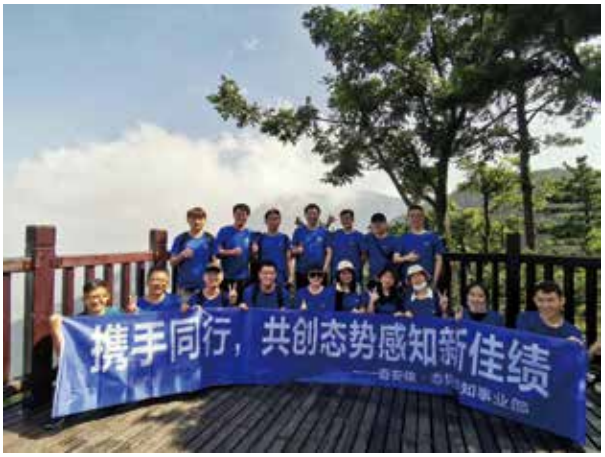
要么不干，要干就干好

从 2015 到 2020 年，常月亲身经历了奇安信监管类态势感知所有的重要时刻，有辉煌的战役，也有迷茫的阶段。

“我们的产品面向的都是监管类头部客户，战略意义不言而喻。但它不是合规类产品，没有标准，不可能开发后一劳永逸，它是一套动态变化的解决方案，要跟着国家政策走、跟着客户职能的不断演进走、跟着客户上到省部级领导下到基层不同科室科员的差异化需求走，而且往往需求提出时很模糊，但要求上线的时间窗口又经常以‘天’为计数单位，所以团队经常要调整设计方案、进行非常快速的迭代开发，通宵达旦是家常便饭。而且每到节假日，往往是监管客户业务繁忙的日子，态势团队经常需要提供现场支持，随时待命”

图：态势感知北京研发团队团建合影

因为加班强度大，产品不确定性强等原因，2017 年 7 月，态势感知团队出现人员流失危机，连常月在内，只剩 10 人。齐总亲自召集所有其他产线负责人开会，



图：态势感知武汉研发团队团建合影

借人支援态势感知。1个、2个、3个，全公司一共筹来了19人。副总裁李虎接手态势感知。

“那是我职业生涯的一次蜕变，二选一的时刻，我选择了留下。然后我就想，要么不干，要干就干好！”

坚定了信念的常月，在李虎的领导下，带着团队重装出发。因为业绩突出，2019年，常月由研发总监破格提升为事业部总经理。

“我之前是研发思维，总经理这个位置对我来说，有很大挑战。但在领导和团队支持下，我边学边干吧，根据团队的特点，也根据公司的发展节奏。”

在此之后，奇安信态势感知取得的成绩有目共睹，而常月对自己，对团队，始终保持着清醒的认识。

“态势感知团队的平均年龄是28岁，包括我自己，我是个80后，我们很符合年轻团队的特点，有热情、有冲劲，肯吃苦，目标明确的话，会一往无前。但团队缺失的部分也和年龄有关，特别是在面对客户侧复杂的、不同层级的用户，沟通有难度、差异化的需求，以及大型复杂解决方案的规划、设计、研发、交付、运营等一系列环节上，经常会踩一些坑。但我觉得踩坑不怕，这是成长的必经之路，只要团队价值观是端正的，持续的进步和改进，就会朝目标越来越近。这几年，我们确实取得了很多战役的胜利，但也有波折的时候，中间也迷茫过，而每次突破自己的办法还是那个：二选一，要么不干，要干就干好！每到关键点，我们做出这个选择，自己和团队就又往前走了一步。”

而虽然工作作风非常硬朗，6岁的女儿安安始终是常月内心最柔软的部分。

忙碌的工作、频繁的出差，让常月错过了很多女儿成长的时刻。

“今年过年的时候，女儿说，妈妈上班很忙，那能不能当妈妈的小尾巴，带自己一起去上班？”

3月21日，奇安信召开了年会，也把这天设为了全国所有办公区的“家属开放日”。安安终于如愿和妈妈一起来“上班”了。

小姑娘看到了一楼的乐高大虎符，也摸了摸二楼的乐高墙。虽然，先进的乐高技术理念在孩子眼中还只是玩具，但和妈妈有关的一切，永远都是那么美好、温馨。安

图：常月和女儿安安

守护奇安信人的安全防线

作者 公关部 张雪丹

1月28日晚10点半，奇安信安全中心3楼西南角，行政部办公区依然灯火通明。

键盘的敲击声、蓝信消息的提示音、电话沟通的声音互相交织：“第一批疫苗接种时间提前到了明天，你最近是否有咳嗽、发烧、身体不适等症状？日常有没有比较明显的过敏症状？可以按时接种疫苗吗？”

由于疫情防控工作的需要，一年以来，行政部的同事已经习惯了各种紧急通知和突发任务，并且能做到快速反应和组织工作，忙而不乱，是这支“娘子军”的“战斗技能”。

纤手筑起防疫“安全墙”

这一次，是原定在春节后开展的西城区新冠疫苗大规模人群接种工作，在当晚7点左右接到紧急通知，我司员工优先安排于第二天进行疫苗接种。此时，距全员疫苗接种通知发布还不到30小时。

行政部紧急统计已报名人数，快速分组后，行政部运营组全员上阵，联系报名员工进行逐一沟通，信息整理汇总。

当晚，那片工位的灯亮到了0点以后。

翌日，沟通确认可以按时接种疫苗的员工被分成了8组，按时间段分批在东大堂集合，每组由行政部3名员工组织带领，从奇安信安全中心步行前往1公里外的疫苗接种点，有序组织登记、排队、接种疫苗，并在接种点观察半小时、确认无恙后，再回到公司。

这样的往返，负责组织疫苗接种的行政部同事，每人当天都至少跑3、4个来回。在晚上6点前，完成了第一批275名员工的疫苗接种，并确认大家暂无不适之后，她们才松一口气，坐下来歇一歇跑了一天已经浮肿的双脚，放松一下奔波一天而酸痛的腰背。

不过，休息也只是短暂的。

春节假期后，第一批接种疫苗的同事需要及时安排接种第二针疫苗，以保证防护效果；安服部门要在3月

为全国两会提供网络安全保障工作，团队希望可以在会前为会议保障团队完成疫苗接种，以保证员工在工作期间的防疫安全；春节假期期间防疫物资采购、储备，防疫工作计划制定；春节返乡过年员工的防疫工作计划制定……

一桩桩一件件，写满了行政部的工作计划表。

防疫重要 员工感受同样重要

第一次疫苗接种的高效有序，也得益于一周前的另一次紧急任务组织。

1月22日上午9点半，行政部朱映雪开完晨会后，正在梳理当天的工作内容，突然接到社区的紧急通知：奇安信安全中心全体员工需于当日10点到展览馆前广场参与核酸检测。

安全中心办公区常驻办公人数1700余人，核酸检测涉及公司内部的员工组织和外部与社区、街道管委会等部门的对接。即使是10人一组混检，也是非常庞大的工作量。

紧急开会，制定组织工作方案，编写通知内容及核酸检测预约操作说明，发布全员通知后，就马不停蹄地开始组织员工登记、排队，引导前往检测地点。

为了避免员工大量聚集，行政部同事疏导员工先去吃午饭，然后分时段到东大堂集合，自己却是忙到水都喝不上。但由于此次核酸检测是西城区统一组织的大规模核酸检测，附近街道及社区居民也都会参与检测，检测点预计需完成10万人次的核酸检测，大量人群聚集的状况难以避免。

尽管有公司党员志愿者的帮助，2个多小时过去，也仅有100多位员工完成了检测。冬日的午后，尽管还有些许的阳光可以带来暖意，但北京地区腊月的寒风依然让待在户外的人们缩手缩脚。

天气寒冷、检测效率低下、人员聚集风险增加，行政部日常负责对接街道、社区工作的洪小霞，主动联系社区，申请在奇安信安全中心增设临时检测点，邀请医护人员上门进行核酸检测，避免人群大量聚集，也可提高检测效率。同时，安排物业人员，提前布置检测空间、准备所需物资等。

在反复沟通和协调下，当天下午3时，社区同意在公司设立临时检测点并安排3名医护人员上门，为安全中心员工进行核酸检测。检测工作效率大幅度提升：截止晚上8点，奇安信安全中心楼内近1600名员工核酸检测顺利完成。

安全快一步 安全每一步

一年以来，奇安信北京地区所有员工进入办公区出示健康宝、测量体温、佩戴口罩已经成为日常流程；食堂就餐，大家也习惯了餐厅限流、就餐时对角落座；开会沟通时，主动保持距离，佩戴口罩，个人防护已经成为了大家的日常生活习惯。

而在更多大家不太注意的地方，是行政部制定防疫工作计划，安排物业人员通风、清洁、消毒、采购防疫物资、张贴防疫工作提醒；接待上级单位的防疫检查，根据检查结果制定工作改进方案并落实工作，一年以来，仅北京地区接待上级各单位防疫安全检查 60 余次；关注全国各地疫情信息动态，及时对内部员工进行活动范围调查，与人力部门一起，根据各地防疫工作要求，安排中高风险地区员工的居家隔离、核酸检测等工作……

“安全快一步”，不只是开展网络安全工作的理念，更是落实在了奇安信人工作的方方面面。

节后返京员工均平安顺利完成了核酸监测和健康观察；安服部门两会网络安全保障团队在会前顺利完成了疫苗接种，并圆满完成工作任务；公司员工的疫苗接种工作有序推进，并为员工争取到了专场接种，高管团队带头接种、带头动员。经过前后 4 批次的集中接种，截至 3 月 22 日，奇安信安全中心楼内员工 1855 人，有 1533 人进行了疫苗接种，接种率达 83%。

3 月 24 日，西城区聂杰英副区长为奇安信授予了楼宇新冠疫苗“应接尽接”绿色标识，成为金科新区核心区首座挂出该标识的楼宇。

行政部“娘子军”用纤纤素手，为奇安信人筑牢内部的“安全底板”，践行着奇安信人的安全承诺。安


让网络更安全
让世界更开
10:04:11

摄影师：奥运中心 金孟忱

实战攻防演习期间，奇安信应急响应中心成立了战时指挥部，研判专家、安全服务工程师、产品、技术工程师 7x24 小时待命，随时处理安全事件，为一线攻防人员提供技术支撑。

大事记

建网安新生态共享万亿市场红利 奇安信举办2021分销商大会

4月16日，全国各地近百家核心分销商参加了“网安一哥”奇安信在京举办的“2021奇安信商用市场分销商大会”。奇安信董事长齐向东、总裁吴云坤、高级副总裁曲晓东、副总裁刘进出席并发表讲话。

奇安信在2014年成立之初，便开始探索适合奇安信业务发展的渠道建设。2017年，奇安信正式提出了渠道化战略，把渠道建设和发展作为一线业务发展最重要的工作之一。2020年，奇安信步入高质量发展阶段之后，渠道化战略将持续作为核心战略推进。

目前，奇安信的合作伙伴已经覆盖全国所有省份，在全国各地发展了将近2000家合作伙伴，共同拓展网络安全蓝海市场。

奇安信参与编写的金融数据安全生命周期规范日前正式发布

近日，由奇安信科技集团股份有限公司、深圳云安宝科技有限公司全程参编的《JR/T 0223-2021 金融数据安全 数据安全生命周期规范》由中国人民银行正式发布。此规范指导金融业机构合理制定和有效落实金融数据生命周期管理策略，进一步提高金融业机构的数据管理和安全防护水平，确保金融数据安全应用。

《规范》给出了数据生命周期安全框架遵循数据安全原则，以数据安全分级为基础，建立覆盖全数据生命周期过程的安全防护体系。

全国工商联党组书记徐乐江一行到奇安信开展专题调研

近日，中央统战部副部长、全国工商联党组书记徐乐江一行莅临奇安信集团，与奇安信集团董事长齐向东等公司高管进行了深入交流。全国工商联副主席黄荣、中央统战部非公有制经济工作局局长张天昱、副局长陈浩、全国工商联经济部部长林泽炎、宣教部副部长李晓兵等参加调研，奇安信总裁吴云坤、高级副总裁曲晓东等陪同交流。

4·15 全民国家安全教育日活动走进校园 奇安信在北京三十五中开讲

在第6个全民国家安全教育日来临之际，奇安信随西城区委、区教育工委组织的“4.15”全民国家安全教育日进校园活动，为北京市第三十五中学的学生们上了一堂生动的网络安全教育课。

活动现场，西城区区委常委、政法委书记姜立光为齐向东颁发了西城区委网络安全顾问聘书；三十五中党委书记孔燕为裴智勇颁发了北京市第三十五中学网络安全教育导师聘书。

政校企三方联动 重庆市网络安全人才培养计划正式启动

由重庆大学、西南大学、重庆邮电大学等 10 所院校联合发起的重庆市网络安全人才培养计划启动大会在重庆青年职业技术学院举办。

重庆市网络安全人才培养计划是在重庆市委网信办的指导下，由奇安信集团作为技术支撑单位，组织重庆市范围内知名院校共同启动的网络安全培养计划。拟组建“重庆市高校网络安全战队联盟“，打造全国首个城市级的网络安全人才培养模式，增进各院校和企业之间的互动交流，推动网络安全技术和人才培养模式创新，在学生群体中培养一批具有“实战经验的高水平网络安全攻防队伍”，持续提升全市网络安全攻防技术水平。

奇安信与德阳市政府达成战略合作 共建西部特色网络安全之城

4 月 9 日，在德阳市委书记靳磊和奇安信总裁吴云坤等领导的共同见证下，德阳市人民政府与奇安信签订战略合作协议，双方将在德阳市数字经济产业发展、网络安全等领域进行合作，大力发展网络安全产业生态，推进德阳数字经济发展。

根据协议，双方合作构建 "141 发展工程 "，助力德阳全面提升网络空间安全治理能力的同时，大力发展基于大数据协同创新的网络安全产业生态，尤其在工业互联网安全领域，双方将积极争创国家工业互联网安全创新示范园区，创新工业安全人才培养模式，共同打造西部工业安全人才输出高地。

奇安信集团与工信部电子五所达成战略合作

4 月 8 日，奇安信集团（688561.SH）与工业和信息化部电子第五研究所（中国赛宝实验室）签署协议，双方达成战略合作伙伴关系，约定根据自身优势资源，在党政军、社会团体和企事业单位等网络安全与信息化有关业务领域开展业务合作、科研课题及技术研究合作。

根据协议内容，奇安信集团与工信部电子五所将面向政企客户的需求，融合双方的优势产品和服务，设计联合解决方案。双方将结合自身科研基础及优势，重点在云计算、大数据、网络空间安全、信息技术创新应用等方面开展相关科研课题的研究合作，对相关领域课题展开前瞻性技术研究探索，深入进行联合申报、专题合作项目以及国家信创入围等方面的工作，同时提供相关技术支持和咨询服务。

奇安信团委正式成立

3 月 31 日上午，共青团奇安信科技集团股份有限公司团委委员会第一次团员大会在奇安信安全中心多功能厅举行。

作为属地非公企业，奇安信集团根据街道团工委批复成立共青团组织，在集团党委带领下成立大会筹备组，召开了第一次团员大会选举团委委员。本次大会采取差

额选举、不记名投票方式选举产生了共青团奇安信科技集团股份有限公司第一届团委委员，随后，召开了新一届委员会第一次全体会议，选举产生了书记、副书记，明确了委员分工。

奇安信 &Gartner 最新白皮书《安全运行迎来 SOAR 时代》发布

近日，奇安信 &Gartner 最新白皮书《安全运行迎来 SOAR 时代》正式发布。《白皮书》显示，随着网络空间安全对抗的持续升级，当前企业和组织的安全运行工作在人员组织、告警处置、快速响应、知识沉淀、整合协作五个方面面临的挑战越来越突出，安全运行呈现安全能力编排化、安全流程自动化、安全运行臂闭环化的趋势。为了应对这些挑战，安全编排自动化与响应（SOAR）应运而生，安全运行迎来 SOAR 时代。

清华大学 – 奇安信联合研究中心打造产学研深度融合典范

清华大学（网络研究院）– 奇安信集团网络安全联合研究中心（以下简称联合研究中心）研究成果汇报暨管委会扩大会议在清华大学举行。

该联合研究中心于 2019 年 1 月成立，利用清华大学网络研究院的学术研究和技术开发实力，结合奇安信集团的行业与产业优势，围绕互联网基础设施和协议安全、检测分析与数据驱动安全、物联网 / 车联网、5G 等新兴网络安全、移动通信系统安全等重点课题开展深入研究。

自成立以来，联合研究中心在安全领域发表国际顶会论文 10 多篇，其中 2 篇获最佳论文奖；联合申请技术发明专利 22 项；出版专著《互联网基础设施与软件安全发展报告》；在互联网基础设施 DNS 和 CDN 安全、APT 攻击及防御等方向支持国家重要需求，承担 6 项国家科研课题；联合组织两届大数据安全竞赛 DataCon，吸引顶级高校和企业参赛并获奖；多次联合组队参加 GeekPwn、天府杯、工业互联网安全技术大赛等安全竞赛，获重要奖项 9 次。

奇安信安全中心成金科新区首座授予新冠疫苗“应接尽接”绿色标识楼宇

3 月 24 日，西城区聂杰英副区长为坐落于北京市西城区金科新区的奇安信安全中心授予了新冠疫苗“应接尽接”绿色标识，这也是金科新区核心区首座挂出该标识的楼宇。

市政协副主席、市工商联主席燕瑛对奇安信集团积极响应党委政府号召，落实防疫责任，主动实现集团员工“应接尽接”表示高度肯定。

发挥企业科技创新主体作用 北京市工商联到访奇安信并组织专题调研

为贯彻落实党的十九届五中全会和中央经济工作会议作出的“强化国家战略科技力量”重大决策部署，北京市工商联围绕“发挥企业科技创新主体作用，壮大国家战略科技力量”主题开展专题调研。北京市工商联一行走进奇安信，参观奇安信应急响应中心和安全能力演示中心，了

解奇安信参与 2022 年冬奥会和冬残奥会情况，并与奇安信、恒华科技、安博通科技、赛微电子、唐杰科技 5 家民营科技企业代表座谈交流，听取企业科技创新方面的问题和建议。

“网安一哥”上市后首次云年会

在奇安信集团 3 月 21 日举行的“云年会”上，全国 30 多个省市区 60 多个分支机构和办公区，超 1 万名员工和家属共同参与。中国电子信息产业集团副书记曾毅特邀出席并致辞。

董事长齐向东做了“为梦想全力奔跑”的演讲：“2020 年，全体奇安信人携手并肩，克服疫情等不利条件，顺利登陆科创板，并实现收入 41.64 亿元，同比增长 32.04%。未来十年，网络安全行业将有 20 倍增长空间，我们要加快五五制和干部五条等管理改革落地，为高质量发展夯实基础。”

本次年会，隆重表彰了虎符之星（最佳员工）、扬帆之星、虎符之将（最佳干部）、金砖奖、虎符之军（最佳团队）、建党百年优秀党员奖等先进个人及团队。

作为奥运历史上第一家网络安全赞助商、北京冬奥官方网络安全服务和杀毒软件赞助商，年会特意拿出 2022 年北京冬奥会开幕式和闭幕式门票，作为特等奖和一等奖进行了现场抽奖，获得者可以获得带薪休假，亲临冬奥会现场，在家门口见证这场载入史册的体育盛事。

赛迪报告：威胁检测与响应市场增长率达 51.9% 奇安信天眼市场份额第一

赛迪首次发布《中国威胁检测与响应产品市场研究报告（2020）》，《报告》指出，当前我国威胁检测与响应市场规模高速增长，2019 年市场规模达到 18.2 亿元，增长率高达 51.9%。预计在 2022 年，威胁检测与响应产品市场规模将达到 49.6 亿元左右，并保持持续增长趋势。在国内威胁检测与响应产品市场的主要厂商中，奇安信天眼凭借其在网络安全领域的综合实力及渠道能力，以 15.3% 市场份额位列第一。

荣誉墙

奇安信代码安全实验室协助微软修复远程内核级漏洞 获官方致谢

奇安信代码安全实验室研究员为微软发现三个漏洞（CVE-2021-28445、CVE-2021-28328 和 CVE-

2021-28323），其中 CVE-2021-28445 是“严重”级别漏洞。奇安信代码安全实验室第一时间报告并协助微软修复漏洞。北京时间 2021 年 4 月 14 日，微软发布了补丁更新公告以及致谢公告，公开致谢奇安信代码安全实验室研究人员。

奇安信零信任安全项目获我国智能科学技术最高奖

4 月 10 日，我国智能科学技术最高奖“吴文俊人工智能科学技术奖”十周年颁奖盛典正式召开。其中，由奇安信集团完成的“支撑零信任安全架构的人工智能信任决策系统”项目，荣获第十届吴文俊人工智能科技进步奖（企业技术创新工程项目）。

“吴文俊人工智能科学技术奖”是我国智能科学技术领域唯一以享誉海内外的杰出科学家、数学大师、人工智能先驱、我国智能科学研究的开拓者和领军人、首届国家最高科学技术奖获得者、中国科学院院士、中国人工智能学会名誉理事长吴文俊先生命名，依托社会力量设立的科学技术奖，被誉为“中国智能科学技术最高奖”，代表人工智能领域的最高荣誉。

奇安信荣获中国智能网联汽车技术创新成果奖

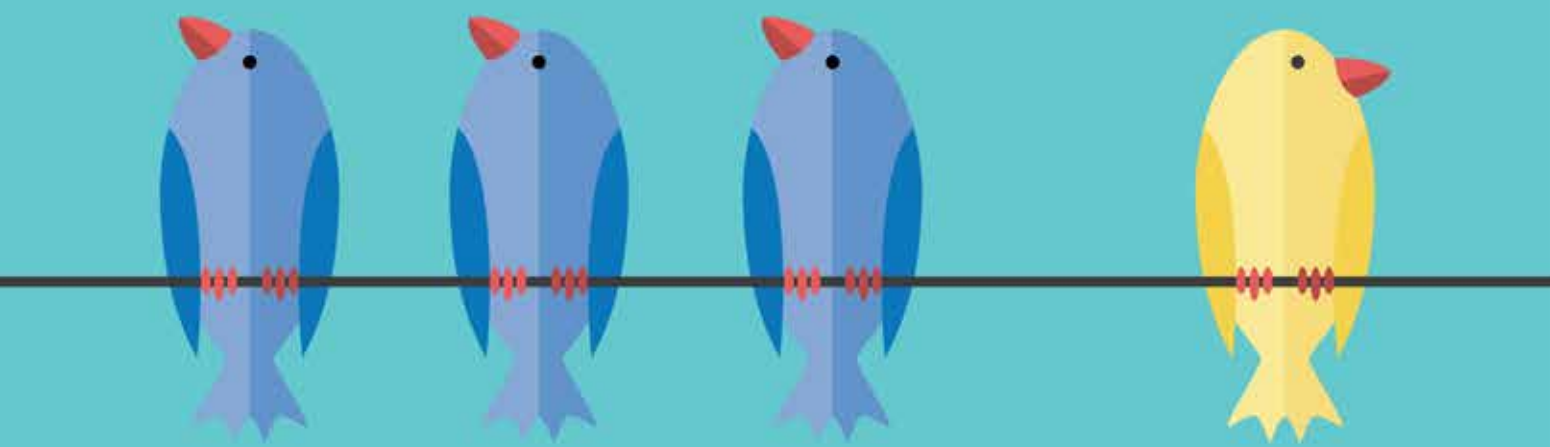
4 月 1 日，由中国汽车工程研究院股份有限公司、中国汽车信息化推进产业联盟、江苏智行未来汽车研究院共同主办的“中国智能网联汽车创新成果大会”在南京举办，奇安信集团荣获“中国智能网联汽车技术创新成果奖”，标志着奇安信在车联网安全领域再次获得行业肯定。

IQ 战队夺魁 RHG 国际机器人网络安全对抗赛

由奇安信技术研究院星图实验室和中科院软件所可信计算与信息保障实验室ISA研究组联合组成的IQ战队，在“纵横杯”网络安全竞赛总决赛 RHG 智能漏洞挖掘赛道中荣获冠军，并在两个赛题上获得一血（第一个解题）。

RHG（Robo Hacking Game）国际机器人网络安全大赛类似于 2016 年美国 DEF CON 引入的 CGC（Cyber Grand Challenge）赛事，整个比赛由自动攻防机器人系统自主完成，全程无人工参与。目的是促进程序分析及漏洞挖掘相关前沿技术在自动攻防场景中的应用，提升其在真实场景下对软件漏洞的自动发现和利用能力，推动网络安全相关攻击和防御技术的发展，发掘和培养人工智能攻防人才。

密码要安全又独特!



选择的密码要易记、但又难猜。使用短语可以实现强密码，做到易记又难猜。比如，工作996让家人666

网络安全意识海报（密码安全）来源于网络

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信图书馆

网络安全科普系列

网络安全实战系列

国际经验分享系列

网络安全认证系列

网络安全教育系列

扫码购书

奇安信致力于网络安全科普、教育、认证与实战，基于国内外先进实践及理念，编撰并翻译系列网络安全丛书。

奇安信

奇安信威胁情报中心

中国威胁情报行业领军者

奇安信威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

威胁情报中心

威胁研判分析平台ALPHA： 一站式云端SaaS服务的威胁分析工具平台。是安全分析师为同行打造的利器，针对IOC查询、线索关联、事件溯源、样本行为检测和同源分析等威胁分析场景提供全面的解决方案。

高对抗云沙箱分析平台： 提供多种动静态检测、分析技术，展现文件各方面特征，帮助分析师快速判别、并掌握恶意软件的详情。

威胁分析武器库： 服务于安服、安运、安全分析师及各类企业用户。支持IOC自动化数据流检测、失陷情报、恶意IP批量查询；支持邮件批量自动化检测；支持WEB应急日志、主机应急日志分析。

威胁情报系统QAX TIP： 威胁情报平台是情报收集、维护、使用的综合性平台。可帮助企业在安全运营中，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁，并分析产生行业威胁情报。

威胁雷达： 利用大数据和威胁情报监测技术，整合了奇安信的高、中位威胁情报能力，提供指定区域内网络威胁高位监控、案件拓线分析、样本深度分析等多种能力。

样本同源分析系统： 奇安信威胁情报中心红雨滴团队基于样本基因深度解析，使用机器学习算法用于APT数字武器追踪的可视化分析系统。

高级威胁分析服务： 为网络安全主管单位，政府机构、行业客户及高校科研机构提供情报线索拓线和威胁分析服务，输出深度分析报告供其决策参考。

奇安信威胁情报中心：
ALPHA网址：https://ti.qianxin.com
雷达网址：https://r.ti.qianxin.com
扫描关注我们的微信公众号
邮箱：ti_support@qianxin.com

奇安信

新一代网络安全领军者

聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证

态势感知解决方案市场领导者——IDC认证

态势感知技术创新力和市场执行力双第一——数世咨询认证