ISC 2023

ISC数字安全创新性案例报告

CONTENTS 目录

聚能安全创新 · 服务数字安全

—— ISC 2023数字安全创新百强评选活动

在这个信息化飞速发展的时代，数字安全已经成为了国家安全、社会稳定和经济发展的关键支柱。随着技术的持续进步和应用的广泛扩展，数字安全面临的挑战也日益严峻。在这样的背景下，ISC 2023数字安全创新百强以“聚能安全创新，服务数字安全”为主题，致力于搭建一个交流分享的平台，推动数字安全领域的创新和发展。我们期待通过这个平台，激发更多创新思维、共享成功经验，让数字安全从挑战转变为全新的机遇。

这是一个以服务数字安全为主旨的时代，我们迫切需要前瞻性的创新，以确保数字社会的安全和可持续发展。因此，“聚能安全创新，服务数字安全”不仅仅是一个主题，它是对当前数字安全领域的深入洞察，也是对未来发展方向的明确指引，更是我们面对新形势、新挑战时的行动号召。

“聚能安全创新”意味着集结各方力量，汇聚创新思维，共同推动数字安全技术的发展。它强调的是一种集体的力量，一种跨界合作的精神，一种不断探索和前进的态度。在这个主题下，我们鼓励和支持各行各业的企业投身到数字安全的创新实践中，通过技术创新和模式创新，提升数字安全的整体水平。

“服务数字安全”则是我们创新的最终目的，创新不是为了创新本身，而是要服务于社会，保障数字世界的安全运行。这需要我们不仅要关注技术的先进性，更要关乎技术的实用性和普及性，确保创新成果能够真正落地，服务于客户。

本次ISC数字安全创新百强案例评选活动就是在这样的背景和主题下发起的，通过这次活动，我们将深入挖掘那些突破性的案例，深入剖析这些案例的背景、实施过程、创新点以及所带来的影响。这些案例承载着创新的火花，我们期望通过这些案例能够为读者提供一个全面、深入的数字安全创新视角，为未来的数字安全发展提供借鉴与启示。

此外，ISC还为入选企业量身定制了独特的雷达图，这些雷达图涵盖了五个关键维度：技术创新能力、行业影响力、研发投入能力、经营能力以及市场拓展能力。ISC专家团队将依据企业提交的详尽数据和案例分析，进行综合评分，最终形成展现企业全方位实力的雷达图。

这些雷达图不仅直观地展示了企业在数字安全领域的综合实力和特色，还为行业内外的观察者提供了一个评估和比较的工具。通过这种方式，企业可以清晰地识别自身的优势和潜在的改进领域，同时也为投资者和合作伙伴提供了决策参考。

通过这种创新的评估，ISC数字安全创新百强评选活动旨在激励企业持续推动技术边界，加大研发投入，优化经营策略，并在全球市场中扩大影响力。这不仅是对入选企业的认可，更是激发整个行业追求卓越的动力。我们期待本次推出的雷达图能够成为企业成长的路标，引领数字安全行业向更高的目标迈进。

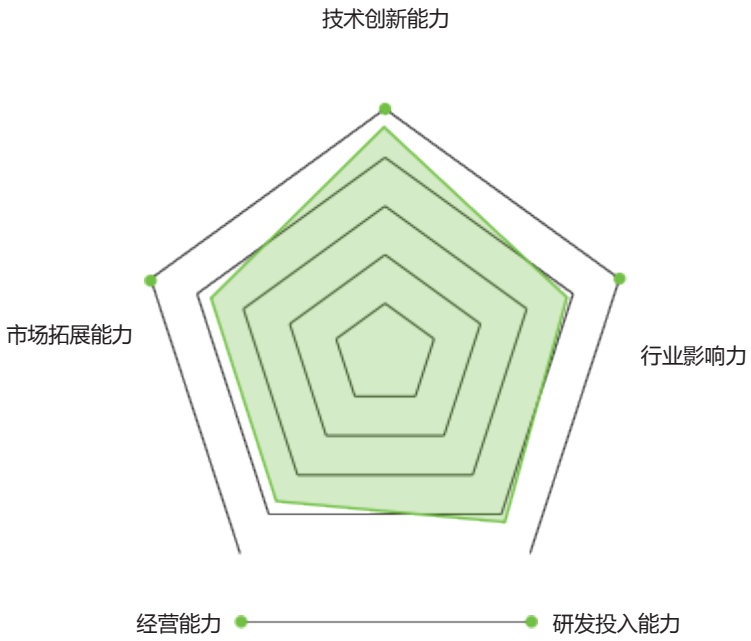
“ISC 2023数字安全创新性案例”入选结果公布

序号	案例提供方	案例名称
1	亿格云	小红书基于零信任SASE办公安全一体化解决方案
2	薮猫科技	三一集团&薮猫科技-智能制造业数据安全建设案例
3	360数字安全集团	某新零售集团股份有限公司安全运营服务项目
4	悬镜安全	基于代码疫苗技术的某运营商SCA开源治理实践
5	齐安科技	电力监控系统站端运维接入安全解决方案
6	众智维科技	能源行业工业互联网安全智能应急响应平台建设
7	观成科技	金融行业加密业务安全运营平台建设项目
8	金睛云华	金睛云华助力某央企高级威胁检测能力建设
9	未岚科技	某证券公司网络资产攻击面管理平台建设方案
10	牧联链	基于区块链和人工智能技术的畜牧肉牛产业全流程服务平台建设

02

亿格云

- **企业定位：**办公安全一体化解决方案领导厂商
- **企业介绍：**亿格云是SASE安全服务商，自主研发了SASE服务平台—亿格云枢，提供包括零信任网络访问（ZTNA）、数据防泄漏（XDLP）、威胁检测响应（XDR）、防病毒（EPP）、上网行为管理（SWG）和统一端点管理（UEM）等功能，解决企业数字化转型过程中遇到的混合分支办公安全、数据安全、终端安全等问题，亿格云已服务超200家上市公司和独角兽企业等在内的行业客户，包括吉利控股、海亮集团、零跑汽车、小红书、美图、奈雪控股等多领域头部企业，在多等行业得到客户认可。
- **重点产品：**零信任数据安全SASE平台-亿格云枢
- **企业网站：**https://www.eaglecloud.com
- **企业雷达图：**



企业案例

小红书基于零信任SASE办公安全一体化解决方案

案例背景：

小红书作为面向年轻人网络购物和社交平台的互联网公司，员工近万人，分布上海、北京、武汉等地，多地远程多设备成为常态，小红书自身对数据分析和安全风控有较好基础，如何在混合办公环境对核心数据防护同时实现高效灵活成为最大挑战，例：①多身份角色，导致管控策略多样化②多终端类型，导致技术方案无法复用③安全产品碎片化，不同环境使用差异性较大安全产品，无法统一管理，平台兼容性差④运维压力大⑤多Agent导致用户体验下降⑥混合办公场景下远程办公让数据暴露面变大。

关键挑战：

01 **多身份角色，接入用户多样化导致访问控制权限难管控：**

除了内部员工，还有大量合作伙伴需要访问内网应用。不同组织和人员的访问权限划分需要实时更新，耗费大量精力。

02 **多终端类型，云桌面和沙箱等方案无法适用于所有场景：**

如今办公终端类型多样化，除了常见的Windows、MacOS等PC设备，还有大量iOS、Android等移动设备需要接入办公，传统的数据防泄漏方案无法满足小红书多样化办公设备场景。

03 **安全产品碎片化：**

为了解决不同安全问题，需要部署多套产品。不同产品有不同的管理平台，运维人员需要适应不同产品的设计逻辑和操作习惯，在不同产品控制台之间频繁切换，学习成本高且维护压力大；此外，各个产品之间无法形成联动处置。

04 **传统安全产品开放性低：**

在OpenAPI和自定义分析能力方面无法灵活匹配小红书业务，导致1+1＜2；且传统的安全产品标准化交付模式，在一些细分场景下无法匹配小红书业务，共创定制需求响应慢，甚至无法完全满足。

05 **终端安装多个Agent默认就占用大量资源，导致员工办公体验差：**

传统办公安全解决方案，需要安装VPN、EPP、EDR、DLP、UEM等多个Agent，会占用大量设备资源，影响员工办公体验。

06 **混合办公场景下远程办公让数据暴露面变大：**

快速发展的小红书，灵活办公场景随处可见。混合办公场景下各接入点的安全水位不一致，容易成为攻击者的目标。

07 **数据安全法律法规发布，企业敏感数据难管控：**

随着《个人信息保护法》等法律法规发布，企业的敏感数据面临监管压力，但如今敏感数据分布广，获取方式多样，外发通道难以管控，给企业带来了挑战。

解决方案：

小红书与亿格云基于SASE共创零信任办公与数据安全一体化解决方案：

o BeyondCorp与SASE能力的结合

小红书早期调研了以谷歌的BeyondCorp为代表的零信任方案，其无端的访问方式确实带来了极致的用户体验。安全团队可以在网关上实现各种风控能力，然而BeyondCorp也存在很大的缺陷：

1、协议兼容性较差，只支持七层流量；

2、需要对外暴露HTTP(S)服务，存在较大的攻击面；

3、缺少终端安全管控手段，无法覆盖终端的安全问题；

4、实现高可用需要投入大量时间、精力和成本。

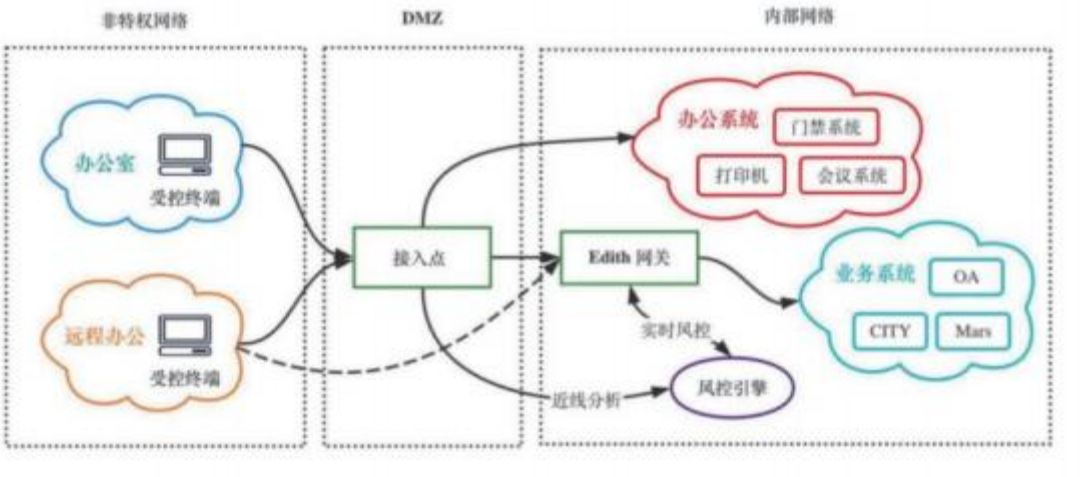
于是小红书关注到近年来的零信任新趋势，即 SASE架构，它天然弥补了上述几个缺陷，分布式的POP点确保系统天然高可用，也补充了客户端的安全管控能力。然而，直接使用SASE也存在弊端， 无法利用小红书自有业务网关优势，更要放弃小红书在网关上积累的风控能力，与企业内部的数据管理脱节。

综合调研了各种方案后，小红书根据自身网络架构特点，提出了一个创新的想法，将BeyondCorp与SASE能力结合，完美地满足了终端、网络和身份的安全需求。

1、终端 - DLP、杀毒、零信任访问等功能All in One，并且支持终端安全与访问控制策略联动；

2、网络 - 办公网改造成非特权网；全球POP接入点实现高可用；

3、身份 - 客户端与身份绑定，并在网关处与请求身份匹配，解决身份盗用问题；

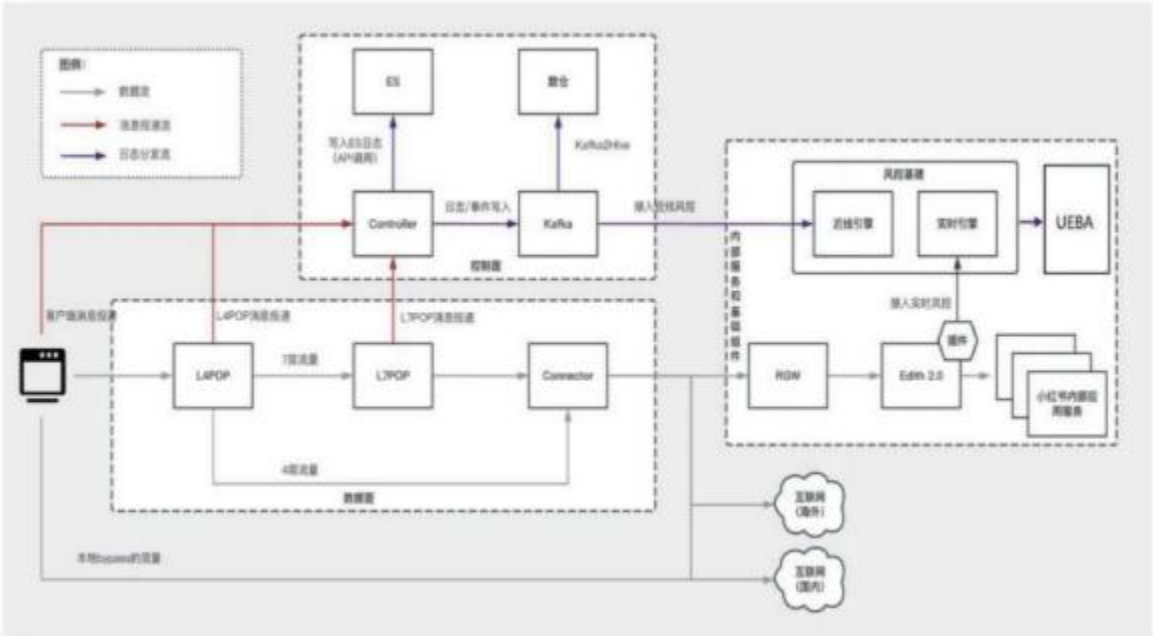


网关与客户端联动

在以往依赖网关实现的风控方案中，网关无法拿到终端的安全信息。小红书创新地将网关风控与客户端联动，网关风控能实时识别请求中是否包含客户端信息并检测客户端状态，确保终端的可信性。同时，还可在终端上实施各种安全合规策略。对于未安装客户端的访问请求，网关风控可将用户跳转到客户端下载页面，以低成本实现客户端全员覆盖。

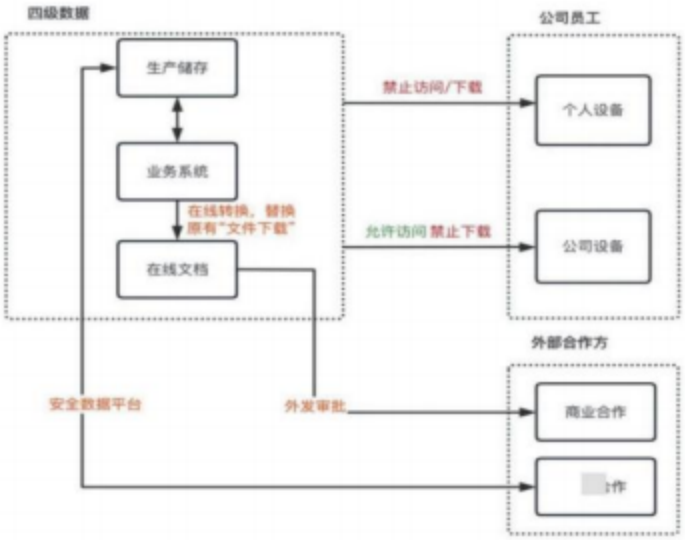
实时风控和异常分析

小红书在风控基建上持续投入了多年，建立了完善的数据安全和风控体系。这套零信任访问系统可以将4/7层日志和客户端日志接入风控系统，实现与风控系统的无缝结合。客户端采集的安全信息为风控系统添加了更多维度的数据，实现更加精准和完善的异常分析。



红线数据不落地

小红书从数据安全生命周期管理出发，以“不落地”实现红线数据不泄露。在内部，小红书严格执行数据分类分级/API安全/脱敏/权限管理等措施， 以数据打标和API打标作为数据防泄露管理的起点。对于内部生产类数据，将数据管控手段左移，通过在线转换业务系统产生的文档，使用在线文件取代文件下载。



相比传统沙箱隔离和文件加密方案，这种做法不仅安全性更高，而且员工有更好的使用体验。

多级容灾机制

整个访问控制系统是串联在访问过程当中，一旦出现故障将影响所有员工的正常办公，所以系统的稳定性是小红书考虑的重中之重，为此小红书与亿格云创新性地打造了一个多级容灾方案。

默认情况下，流量通过小红书自建的私有POP节点，确保流量和数据都在自己可控的网络环境中。当本地POP节点发生故障时，系统可自动切换到亿格云的公有云POP节点。这种容灾方案已经可以保证超高的可

用性，但是小红书不满足于此，在此基础上还实施一层Wireguard方案，当零信任防护模式失效时降级到 VPN模式，以此实现更高的可用性。

- **自研客户端**

小红书向员工展示自有品牌的办公安全平台，以增加员工对安全软件的认可度，同时还可以在客户端上集成更多内部常用的办公功能。小红书基于亿格云的客户端SDK，打造了一个匹配小红书自身风格的客户端UI，加之便捷的办公体验，实现其对员工的“种草”。

创新性与优势：

值得一提的是，这一轻量稳定、简洁高效的一体化“内部安全办公系统”为小红书带来的价值已得以显现。在内部调研中，该系统也获得高达70% 的NPS（口碑值）：

能力一体化、管理更精细：

一体化设计思路，即平台/功能/管理一体化，大幅降低终端安全体系建设、运行和扩展的复杂性。管控力度更精细、权限可自动梳理、运维难度更低，对终端、身份、行为和数据等进行全生命周期的精细化准入管控，确保终端符合内外部的相关准入要求，做到合法合规，准入可信。