

证券代码：688225

证券简称：亚信安全

亚信安全科技股份有限公司 投资者关系活动记录表

编号：2022-028

投资者关系 活动类别	<input checked="" type="checkbox"/> 特定对象调研 <input type="checkbox"/> 分析师会议 <input type="checkbox"/> 媒体采访 <input type="checkbox"/> 业绩说明会 <input type="checkbox"/> 新闻发布会 <input type="checkbox"/> 路演活动 <input type="checkbox"/> 现场参观 <input type="checkbox"/> 一对一沟通 <input type="checkbox"/> 其他（请文字说明其他活动内容）
参与单位名称 及人员姓名 （排名不分先后）	开源证券 刘逍遥 诺安基金 左少逸 中信建投 应璩、曹添雨 千合资本 邹珠印 首创证券 傅梦欣 益民基金 关旭 渤海汇金 徐中华、陈海涛
时间	2022年9月20日 14:00-15:00 2022年9月21日 09:30-10:30 2022年9月22日 15:00-16:00
地点	公司会议室
上市公司 接待人员姓名	董事会秘书郑京、董办投关人员、相关业务负责人
投资者关系活动 主要内容介绍	<p>一、 公司情况介绍</p> <p>二、 问答交流</p> <p>问：给运营商提供的IAM产品主要是解决运营商的客户身份访问控制还是解决内部员工的身份管理问题？</p> <p>答：其实两部分都涉及，常规来讲行业内将IAM分为EIAM和CIAM，EIAM是面向企业内部员工，解决内部员工的身份安全管理问题，CIAM是面向外部客户，为了解决互联网开放后、暴露面里这些系统面向客户端的管理能力。</p> <p>第一，以前主要是解决运营商的内部身份安全管理问题，在运营商的复杂网络结构下，解决人员、系统、设备、应用的账号、认证、授权、审计等安全问题。现在运营商侧的IAM已经发生较大的演变，在原来“4A”账号、授权、认证、审计的基础上加了很多功</p>

能，比如访问控制、安全分析能力、AI，已经变成5A、6A的状态，所以运营商的IAM复杂程度比大多数行业的管理都复杂，一旦运营商的IAM体系构建出来后，我们的产品能够覆盖大多数行业的客户需求。

第二，在运营商侧也构建了To C的IAM身份管理体系，比如运营商的掌上营业厅，是用亚信安全的IAM系统在后台做认证识别，产品面向的是运营商C端客户的身份管理。

问：您刚才提到从4A到现在5A、6A，是不是一些上网行为管理、堡垒机这些能力加在里面整体打包给客户？

答：最早对IAM的定义是把身份识别清楚，做最小粒度的权限授权，早期IAM是这个样子，但实际上最小粒度的授权仅是在管理层面，后来我们在技术层面的演进非常大，在直接的行为层面实施控制，所以Access Control发生在多个维度。堡垒机只是在某些协议通道，比如主机网络设备、数据库系统里。那么在一些常规运维系统里有很多身份安全的问题无法用标准协议解决，比如需要更复杂的图形类工具的访问控制能力。

其实整个零信任体系在运营商的建设，包括我们在非运营商客户侧构建零信任体系，是以综合解决方案的方式做的，不是单一产品。IAM、SDP、微隔离是零信任体系里的产品，这些独立的产品要构成综合解决方案，任何一个客户要的不是产品，是要解决问题，这些安全问题都不是一个点能够解决的，是多个同时并发处理的。所以我们在零信任体系中除了SDP、IAM、微隔离，我们补充了零信任评估中心做动态性的评估构建综合解决方案。

问：IAM作为一个基础设施，产品形态是软件吗？

答：目前IAM是软件形态，软件形态构建解决方案的容易程度非常高，比如承载数以亿计的用户。目前客户的信息系统已经开始云化、PaaS化，基于Docker做云原生能力的构建，大量的平台用户基于云原生平台构建多节点、分布式的能力，所以软件化是构建云原生的基础要素。基于目前的基础架构，IAM也在向微服务、云原生部署、自动化、低代码、无代码的方向演化和发展。

问：IAM跟业务系统的紧密程度有那么高吗？

答：它是紧密结合的，现在所有的业务系统已经没有自己独立的账号、几乎没有通道了，身份的安全管理已经被IAM接管，认证能力全部指向IAM，比如当访问业务系统的时候，输入业务系统地址，其实地址已经不是业务系统的，而是到IAM的登录页面，只有IAM做

完双因素认证、身份识别并且确定对系统有访问权限，才会登录到业务系统上，放行赋予权限。所以业务系统跟IAM是紧绑定的关系。

问：公司的研发投入主要是哪些方向？

答：研发投入基本聚焦在我们原有的优势业务上，亚信安全是一家比较稳的公司，我们的发展策略是聚焦我们的优势方向。我们会围绕平台化这个核心点，现在靠单一产品堆砌是解决不了问题的，需要体系化的安全能力。平台作为枢纽能够把核心领域的产品连接起来，汇聚日志、流量、安全告警的数据，通过平台的能力识别威胁，并把处置的联动措施自动下发下去。所以研发的投入方向围绕平台，在平台里能够发挥作用来进行产品的拓展。第二，我们坚持软件特色，要联动响应处置，软件化更容易实现。

问：亚信安全在端点产品市场占有率有11%，再提升的话主要依靠哪些方面？

答：第一，客户对端点安全的需求在丰富化，原先防病毒是核心诉求，现在新增了资产管理、准入控制等等，功能模块在增加，我们的客单价比前两年有明显提升。从国外也会看到这样的趋势，在端点侧形成EPP平台，通过平台的方式把安全能力聚合，给客户提提供端点侧的解决方案能力。所以客户的需求是在增加。

第二，亚信安全比较有优势的是老客户的复购逐步提升。端点产品服务期到期后客户每年都在续费，新客户拓展的越来越多后老客户的贡献是越滚越大的。所以整体看端点产品体系的增速比较快。

问：公司希望非运营商客户收入达到60%的占比，主要靠哪些行业增长？

答：主要是来自能源电力、制造、金融等行业的收入增长。上半年金融行业同比增长100%、制造业同比增长43%、能源行业同比增长80%，这三个行业收入同比增长75%。我们在这几个行业里原先有一定的基础，销售力量在关基行业逐渐深入的扩展。

问：为什么Q2的增长会比Q1加速？

答：整体销售能力的提升，销售队伍从去年下半年开始到今年上半年陆续扩充，销售人员的能力释放取得了初步成效。

问：销售体系的人员组织是如何建设的？渠道建设的进展如何？

答：矩阵式管理，设立了大的行业事业部，同时建立27个省办，省

	<p>办组织中售前、售后、安服、销售的能力都具备，也要负责渠道的拓展和维护。</p> <p>今年上半年渠道整体贡献有一些提升，收入占比也有所提高，但还是直销占比高，这与我们的客户结构有关系，大客户多一些，直销销售覆盖多一些。腰部以下的广域市场会推出渠道版本覆盖，希望未来渠道的收入贡献逐渐提升。</p>
附件清单 (如有)	无
日期	2022年9月23日