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：2022-025

投资者关系活动类别	√ 特定对象调研　　□ 分析师会议 □ 媒体采访　　□ 业绩说明会 □ 新闻发布会　　□ 路演活动 □ 现场参观　　□ 一对一沟通 □ 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）	新加坡政府投资公司（GIC）徐萌、卫景燊 上海冰河资产管理公司 刘春茂 中金公司 李虹洁
时间	2022年7月26日 15:00-16:00 2022年7月27日 16:30-17:30
地点	线上腾讯会议
上市公司接待人员姓名	总经理陆光明、财务总监汤虚谷、董秘郑京、投关人员
投资者关系活动主要内容介绍	**一、 公司情况介绍** **二、 问答交流** **问：去年以来公司在行业客户结构、产品结构等方面调整的主要核心原因是什么？** 答：公司未来要增长，一个是要去向其他行业拓展，另外一个就是要梳理自身产品业务体系的构成有哪些新的增长点。我们的端点产品体系里终端安全、云安全以及高级威胁治理这类产品都是标准化产品，很契合现在客户的安全需求，加大相关产品体系的销售能力，就能带动我们的增长。这在公司2021年度的业绩中，已经有所体现：公司端点安全产品体系收入实现较高比例的增长，毛利率从2020年的75%提升到2021年的78%。 平台化的思路。通常客户买了很多安全产品，但安全运维人员每天面临这么多的安全数据、告警，实际上并没有把这些安全产品较好的使用起来，处理威胁事件的能力没有得到很好的提升。但如果通

	过我们XDR平台联动方案，则能够很好的解决痛点，包括云网边产品体系里态势感知这类的平台产品，能够很好的满足客户的联动需求，为客户搭建整体防御体系，通过平台带动产品、服务的增长，这是主要考虑。 **问：公司在运营商行业的地位如何？核心产品身份安全的发展如何？** 答：首先，从产品业务本身来讲，数字信任和身份安全产品体系以往在我们的收入占比里较高，包括云网边这两大产品体系主要布局在运营商侧。每个运营商大概31个省分公司，三个运营商大概90多个单位，此外还有一部分专业子公司。公司的身份安全、接入安全、DNS等优势产品占比超过60%，实现高增长的空间有限。 另外，身份安全产品体系跟端点产品体系业务特性不同，身份安全要和客户的业务、系统、人员、流程等融合的比较紧密，客制化程度比较高。如果在客制化程度比较高的情况下扩大它的收入规模、从运营商行业走向其他的行业，就要扩充较多人员，交付的压力还是非常大的，所以目前我们在做的就是要把身份做产品化，产品化提升交付效率之后，我们再向其他的行业去做拓展。这是一个调整的过程，未来2023年、2024年身份安全会再度恢复一个好的增长，当然预计它整体的增速可能低于端点产品体系的增速。 **问：从2020年到2021年，营业收入增长较快，利润比较平稳的主要原因是什么？** 答：相比其他行业，网安行业集中度还是要差一些，相对分散，竞争较激烈，安全行业技术迭代特别快，要不断投入。 从自身情况来看，公司历史的盈利水平在行业内还是不错的，2021年净利润较2020年有四个点的增幅，利润率有阶段性的下调，主要是因为2021年公司在研发侧、销售侧的投入比较多，销售费用和研发费用同比有较大的增长。着眼于未来几年发展的考虑，销售能力必须是要补齐的，这是必要的投入；同时，为了维持产品竞争能力，包括未来增长的布局，研发侧合理的投入肯定是必要的。所以这两块投入在2021年都有较大的提升。随着前期投入的陆续见效，预计利润率将逐步回升，未来会恢复到原有不错的水平。 这些变化与我们发展思路和发展策略是相一致的，要进行行业结构和产品结构两个调整，希望在网络安全快速发展的市场里占据更大的份额、达到一个更高的增长速度，必然要有一个大投入的过程。这样的阵痛期在我们的预期之内，为了长远的发展来讲要忍受相对短期的强投入阶段。

	问：下半年的预期如何？全年需求是否会优于去年？ 答：网安行业有一定的季节性，下半年还是大家比较重视的时间周期，是我们的旺季。如果下半年没有出现像上半年时有发生的疫情影响或者突发严格管控情况的发生，预计会比上半年乐观，客户的需求下半年陆续会释放。目前观察，疫情主要影响政府部门，关基行业中大型客户比较稳定；中小行业客户因受疫情影响本身自己的压力大，对安全投入会谨慎一些。 **问：公司平台化的发展道路是什么样的？对于客户有什么样的价值和意义？** 答：我们谈的平台化更接近Fortinet、Palo Alto的风格。现在我们看到客户的生产网络、数字系统发生巨大变化，边界消亡了，基于5G、云、大数据、AI等等应用，数字化转型面临的安全挑战，原来某些单点产品的防御已经无法防得住，客户需要立体防御的能力。威胁攻击在云、网、端都会有留痕，从互联网暴露面攻进来，或者从钓鱼邮件攻进来，它不真正去做恶的时候没法识别；恶意文件通过互联网暴露面、邮件钓鱼进来，在内部企业网络进行流转，潜伏落在终端或者主机上，勒索或者挖矿、窃取数据时会通过非法外联发起攻击指令，这种APT攻击手法仅仅基于原来传统的边界防御根本防不住，某一个点都不足以支撑把整个攻击链条识别明白、不足以找到真实的恶意程序和恶意文件。 刚才讲了这么多环节，平台化是能够基于真实的黑客攻击链条，基于客户的数字化网络中的各个节点、云网边端都要部署相应的产品，这些产品要真正具备威胁发现能力、处置能力、阻断能力、响应能力，所以网络安全往下发展，平台一定是产品能够解耦、安全能力显性化、能力原子化，能够根据刚才讲的攻击链条编排产品，层层设防，对恶意访问和威胁攻击进行发现、分析、关联、处置、响应、阻断，这才是平台化的核心。 这与搭积木、产品化、微定制是两个层面的问题，搭积木或者产品化的平台，实际上是从软件工程的视角做到微定制、产品能力能够复用。而我们谈到的平台化实际上是从网络安全的视角，在攻防哲学思想发生变化之后，客户需要立体的防御能力。从产品销售的角度就是给客户提供一整套解决方案，从产品到安全服务，举个例子，现在都在谈场景化，现在很多客户面临勒索、挖矿等APT攻击事件，最近观察国内勒索事件太多了，几乎每周处理超过20次勒索事件，基于前面谈到的攻击手法和链条，我们的平台化从市场的角度会推出具象化的产品比如勒索盾，有些已经在客户端得到很好的响应，勒索盾会涉及很多产品，比如在企业入口端部署网关类的防毒墙、SDP，基于企业内网中的流量部署APT产品、在邮件侧的邮件

	网关，在主机和终端上部署云主机安全、终端安全，但不是买一堆产品就结束了，那样的话起不到真正作用，要基于APT攻击的手法和链条，真正从数据和指令层面打通，基于攻击链的分析、产品与数据的结合，准确判断是不是勒索的文件，这里面有很多特性，不管是基于attack特性还是基于攻击手法的特性，基于任何一个单品的数据都无法判断，但是几个叠加就能判断了，才能够成功的发现、进行处置阻断响应。 公司会基于各种威胁攻防的场景，提供各种场景下的平台方案。公司最近要发布抗饱和攻击平台方案，这个平台方案中会有一系列自有优势产品和第三方优势产品部署，海量攻击进来之后在网关侧、企业内网流量侧等攻击节点层层降低，保证核心IT资产和数据的安全，将真正的攻击可达率降到最低。基于攻击链和攻击饱和度，层层设防，从网关到企业内网，到相应的终端，甚至潜伏之后的所有节点能够被监测，真正起到主导作用，告知客户整个过程，从告警变成事件，最后被我们的安全运营人员成功的处置，完成闭环，这是我们平台化的核心思想。 **问：关于平台化从公司经营、客户层面有两个问题：平台化方面如果按照公司所说的把产品拆分为标准化的产品和项目制，平台化会更偏向于标准化的产品还是项目制呢？平台化产品预期会更多的应用在运营商这些大的客户，还是会更多在金融、政府这一类行业客户呢？** 答：两年多前公司的战略规划中，非常明确谈到平台化有三种落地形态：一是国外云原生的SaaS化路径，Crowd Strike成功了，我们也在探索；二是产品公司的平台之路，Fortinet、Palo Alto也成功了，我们主要的平台模式也是这个路径；三是项目制的安全中台，在运营商等超大型企业客户有比较明确的诉求，构建中台化的平台。运营商的信息化水平经过20多年的发展比绝大部分行业要高，走的比较快，他们比较接受平台化，运营商在网络安全行业里是最独特的，全社会的传输骨干网络都在运营商，网络从封闭的4G走向5G，基础架构发生了变化，基于这些特性，运营商对网络安全的要求与其他行业是不一样的，所以平台化在运营商的路径肯定会有差异。 在非运营商行业金融、能源、制造、政府等等，我们还是以产品套件平台为主。这些行业很突出的特征是数字化转型较快，数字系统变成新型生产网络，是生产经营必不可少的系统，对安全能力的要求不再是基于合规驱动或者单品堆砌，一定会要求具备真正的立体防御能力，真正解决问题。这类行业客户会成为黑灰产业链的重点

	目标，所以安全能力不得不考虑，平台化在非运营商行业市场空间巨大，单体客户的采购金额越来越大，而且这种现象会越来越多。
附件清单 （如有）	无
日期	2022年7月28日