

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：2022-029

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）	安信证券 夏瀛涛、杨楠 信泰人寿 刘跃
时间	2022年9月27日 13:30-15:00
地点	公司会议室
上市公司 接待人员姓名	董办投关人员
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：投资者比较关注政策推动行业发展的情况，很多人关注近期网安是否会有新政落地，请问公司对行业的感受或者看法怎样？</p> <p>答：首先，跟友商相比，亚信安全有自己的特点，基本上90%的业务是安全软件，未来我们还会延续这样的特点，目前我们是安全软件领域收入是第一的，还会继续保持下去。第二，我们的客户结构关键基础设施行业的客户占比更多一些，除运营商以外，金融、能源电力等行业拓展比较顺利。涉及关基行业的政策给我们会带来更多的影响，如，之前监管政策要求关基行业安全投入占比提升到10%。从国际形势、勒索等网络攻击事件看，围绕关键基础设施行业也更多一些。前两年等保是一个核心的推动力，我们认为现在推动引擎从单一的等保合规驱动向能力建设和等保合规双轮驱动多元化发展。等保是第一阶段，无论是政府还是中小企业，在第一阶段基本上完成了相关的合规要求，逐渐向能力建设去过渡。所以这个过程中客户的需求是个推动力，安全思想从边界防御转向纵深防御、从单一产品堆砌向体系化建设，政策出来后还要看具体的细则</p>

条例以及后面的检查措施等等，政策驱动是网络安全行业的基础驱动力，是中期的影响。

问：从公司角度怎么去区分标准化产品与非标产品？标准化产品快速增长的原因是什么？

答：端点安全产品体系主要是以标准化产品为主，数字信任身份安全和云网边多数是以解决方案类为主，这两类产品在运营商行业收入占比更多一些，有一些产品比如身份安全是可以复用至其他行业的，DNS安全、DHCP安全则是在运营商方面更多一些。端点产品体系包括若干个产品线，终端安全、云主机安全、APT防护等等。

提升标品占比有几个动力因素：一是，客户本身的需求在丰富化，原先客户就买一个防病毒模块，现在单一模块基础上增加了对端点的资产管理、准入控制、安全管理平台、检测与响应等新功能，所以我们发现功能需求在丰富，带来的是客单价的提升。二是，端点类产品主要是基于病毒库、防护规则会持续迭代，客户购买服务期后到期会续费，老客户续费是增长的一大来源，滚雪球一样，再加上新客户的拓展，所以端点产品体系的增速就比较高。三是，我们原先在非运营商行业的销售人员太少，只有一些标杆客户和头部企业客户，虽然占领了头部阵地但是没往纵深去拓展，2021年公司销售人员增加主要就是在非运营商行业，通过新市场带动了增长。这几个方面促成了标准化产品收入占比的提升。

问：疫情对公司的影响如何？公司采取什么样的措施？

答：疫情确实造成了一定的影响。

首先，政企客户特别是中小企业对安全的投入有所放缓。我们觉得当下阶段更要修炼内功，打造业务健康、管理健康、组织健康，通过企业内部的数字化、管理效率的提升，为长久发展做好基础。

第二，我们还是要紧紧抓住关基行业客户，发挥我们的长处，在客户进行网络安全能力整体体系建设的时候提供我们的整体方案能力、实施能力。在这个过程中能否在实施过程中提高效率能力以及上线的速度、响应程度很重要，效率不高的话会造成业务低毛利甚至亏损。亚信安全在运营商行业深耕多年，运营商行业的特点是用户量大、业务稳定性要求强、数据量大、系统也多，对运营商的长期服务锻炼了我们，所以下一阶段我们要发挥优势，帮助客户建立以平台为核心的整体防御体系。

问：想问一下销售端和产品端从策略角度去突破新的行业有哪些打法？

答：亚信安全之前在金融、能源电力、高端制造等行业有一定基础，主要在头部客户和标杆客户，原先没有本地化的销售人员，从2021年下半年起设立了27个省办，原来主要是直接面对头部客户来做，还有大量的腰部客户没有进去，对于我们来讲是有空白。通过设立省办，延伸市场空间，以头部标杆客户做样板，后面往下推能够快速的扩大，有望在2-3年的时间里会成为主要增长引擎，非营

	<p>商行业收入占到60%的目标有可能提前实现，速度有可能比预期要快一些。</p> <p>问：XDR被大家提的比较多，能否介绍一下公司XDR具体的一些功能？</p> <p>答：亚信安全在国内最早提出XDR。从防御思想来讲，原先端点侧是纯粹的被动防护，接着演进到端点需要检测与响应也就是EDR，后来除了端点的检测与响应，在网络侧也需要检测，出现NDR等等。如果从一个完整的攻击链条来看，仅靠单一产品的局部检测响应是无法看到完整攻击的，所以客户的需求诞生了XDR的概念，通过把各个单一产品联动起来，覆盖整个攻击链条来解决安全问题。XDR方案联动了端点、网络、流量、邮件网关等几个重要领域的产品，基本上就是一个相对完整的防御体系。第一要有优势产品的能力；第二要有平台把这些产品的数据汇聚、分析，同时平台再把处置指令下发；第三，除了自己的数据以外还要有威胁情报中心，通过更广的范围丰富威胁情报库。</p> <p>从国外来看Palo Alto、趋势科技等厂商都推出XDR，国内友商也推出了XDR，特点会不一样，因为基因不同，会从不同的产品方向成长起来，有的厂商偏重分析能力、放在流量检测产品上。亚信安全通过平台，更多的联动端点、流量等方面。所以每个公司的产品的特点相对会不一样，未来XDR我们认为是一个方向和趋势，因为着眼点是从整体来帮助客户构建防御体系。</p> <p>问：XDR产品的功能跟态势感知平台有点类似，怎么区分这两个产品？XDR采用什么样的收费模式？</p> <p>答：第一，XDR比态势感知的部署轻一些，态势感知承担的任务和职责较多，建设周期和客户运维来讲相对比较复杂。</p> <p>第二，XDR更多的会基于自己的产品能力去布局，强调产品的互通性，而态势感知则是从客户的所有安全产品的连接上去做。</p> <p>第三，从适用客户来看，态势感知建设周期长、功能对接繁多，一般适合头部大型客户运用，而XDR比较适合腰部及以下的客户，XDR具有轻量部署、开箱即用的优势。所以在目标市场聚焦上XDR和态势感知还是有一些差别。</p> <p>从模式来看，客户选择功能模块，某个模块购买服务期后会续费，陆续基于XDR能力的构建会增购其他产品，有个Upsell的过程。部署方式来讲更多的是本地化部署，后面我们也有云化部署的打算，主要还是因为客户的付费习惯未发生变化以及对数据安全的考虑。未来SaaS化的方式是新的业务模式，我们也在布局探索。</p>
附件清单 (如有)	无
日期	2022年9月27日