

链长经验

国安信息:布局数据安全生态圈 加速实现弯道超车

近期,为了保障国家数据安全,有关部门牵头发起了“信创云国家大数据中心”建设,其中,国安信息安全科技有限公司(以下简称“国安信息”)与另一家公司联合承担研发任务。

信创云国家大数据中心将承接全国重点行业的数据存储,确保数据的安全、统一、规范化管理。国安信息也因为与业内数十家企业建立了深度合作关系,不断完善数据安全系列产品,打造基于数据安全的生态圈而成为名副其实的信息安全产业链链长企业。



一则新闻报道带来产业灵感

2018年伊始,国安信息正式布局分布式存储这个全新赛道。

国安信息相关负责人告诉《中国企业报》记者,当时看到新闻报道说美国的一家实验室已经开始进入这个赛道,我们在研究了对方的技术路线后,敏锐地感觉到他们的技术路线跟中国的国情有很大的差异性,无法适应国内的存储需求。这就是一次机会,历史性的机遇。但是能否把握住这次机遇,很大程度上是由每个公司的基因所决定的。

在国安信息的头脑风暴会议上,诺基亚的例子被屡屡提起。

当年的诺基亚,不能说没有关注到智能手机的技术动向,并且严格意义上讲诺基亚也是最早研发智能手机的厂商之一。但是诺基亚仍然从战略上丧失了这次机遇,主要还是因为诺基亚在传统手机的市场足够庞大,是既得利益者,如果转向智能手机,无疑是一场彻底的革命。否定自己是最难的,革

掉自己的命也是最难的。

“同样的道理,在数据存储的市场,一直以来都是亚马逊、谷歌等国外的公司遥遥领先,占据全球大部分的市场份额。国内的阿里云、腾讯云都是在追赶,我们欠缺一个弯道超车的机会。现在分布式存储正好就是这样的机会。”上述负责人表示。

国安信息的团队结构决定了公司的业务方向。首席科学家有着20年的密码学和10年的存储经验,其余的技术团队都有多年的数据存储开发经验。同时,国安信息在数据存储领域已经累计了240多项专利,其中国内专利200余项,国际专利40余项。在传统的云存储市场,国安信息没有走类似阿里云的路线,而是更专注于加密存储,并很快完成战略布局。

从制造到智造的产业逻辑变迁

从制造到智造,是从国际分工的角度进行产业的战略升级,传统制造依赖的人口红利已经消耗殆

尽,只有进行战略升级,才能继续在国际市场上保持竞争优势。这是一个大的战略方向调整,也关乎着每一个企业的战略抉择。

国安信息相关负责人认为,我们今天无论在哪个领域哪个产业,都需要一定的国际化视野。特别是高新技术产业,要时刻关注国际上的技术动态。早在2018年,国安信息内部就达成了国际化的战略方向,2019年尝试在韩国进行布局,但是并不顺利。2020年国安信息又进入迪拜,在迪拜建立了全球总部。那里的技术团队更加国际化,更容易创新性地去解决问题。

目前,国安信息的分布式存储技术相比于传统的云存储优势有三方面:一是确保数据安全,任何黑客也无法盗走任何用户的数据,且在全球黑客大会验证过;二是确保数据不会丢失,即使存储数据的服务器或机房损毁,数据仍然存在;三是极大降低数据存储成本,分布式数据中心天然具备灾备属性,不再需要重复建设数据灾备中心。

最为关键的一点,数据存储与国家的数据安全密切相关,国安信息打造的分布式存储系统是完全国产自主化的产品,并且作为唯一的一家分布式存储技术服务商进入工信部信创目录。

谈起当前的信息安全形势,上述负责人表示,随着时代的发展,基于密码技术的区块链逐渐声势浩大,数据安全已经成为全球各国普遍重视的问题。近年来,我国政策环境也发生了巨大变化,数据作为新的生产要素被正式列入中央文件,等保2.0、《数据安全法》《个人信息保护法》《密码法》等多项法律法规相继出台,数据安全为大势所趋,列入社会各行各业核心工作建设范围。最近,反互联网平台数据垄断和滴滴事件更是将数据安全问题提升到了新的高度。国安信息正是基于这些情况,开始提前布局信息安全产业链,致力为国家和政府数据安全做出贡献。



行业分析

信息安全产业链上中下游细分图谱

我国信息安全行业起步较晚,自本世纪初以来经历了三个重要发展阶段(萌芽、爆发和普及阶段),产业规模逐步扩张。尤其是近年来,各类网络威胁造成的损害不断增强,带动了市场对信息安全产品和服务需求的持续增长;另外,政府重视和政策扶持也不断推动我国信息安全产业的快速发展。据有关机构预测,我国网络安全行业市场规模2025年将在1200亿元左右,年复合增长率约为16.4%。

近年来,信息安全涉及信息系统的各个层面,细分领域较多,包括安全内容管理、VPN、防火墙、入侵检测与防御等多个产品类型,市场竞争格局较为分散。在我国主流的信息安全产品领域,每一细分市场的主要竞争厂商都在10家以上。尽管行业内厂商数量较多,但由于目前信息安全市场的细分程度较高,单一企业难以掌握信息安全领域的全

部技术,市场总体的品牌集中度不高,市场份额较分散。

我国信息安全行业产业链上游为计算机及密码设备供应商,如计算机软硬件产品、密码机、密码卡、智能密码钥匙等;下游主要是政府、军队、军工、央企、科研院所、金融、能源等行业,以及云计算、物联网等领域的各级用户。

上游方面:目前,我国信息安全行业上游供给稳定,产品价格和企业营收较稳定。根据国家统计局数据显示,我国计算机、通信和其他电子设备制造业营业收入持续增长,2019年营业收入达到113717.6亿元,同比增长4.5%;2020年上半年受新冠肺炎疫情影响,营业收入为51366.6亿元,同比增长2.3%。现阶段,我国信息安全行业上游企业主要有飞天诚信、美亚柏科、深圳兆日科技股份有限公司等。

中游方面:近年来,受下游需

求及政府政策的推动,我国信息安全产业规模不断扩大。数据显示,2019年,我国网络安全行业总收入668.24亿元,同比增长21.11%;网络安全业务总收入594.14亿元,同比增长17.13%;网络安全技术、产品与服务总收入523.09亿元,同比增长25.37%。2020年上半年,疫情对网络安全行业冲击影响明显,但仍有大部分企业保持正增长。现阶段,我国从事信息安全行业的企业主要有长春吉大正元信息技术股份有限公司、安恒信息、左江科技等。

下游方面:下游是对信息安全具有较高要求的应用行业,包括基础信息网络、面向社会服务的政务信息系统、电子认证服务业等重点行业,主要为政府、军队、军工、央企、科研院所、金融、能源等行业,以及云计算、物联网等领域的各级用户。数据显示,我国电子认证服务总规模从2014年

的129.9亿元增长至2018年的322.2亿元,2019年约为360亿元。有机构预测,到2025年市场规模将突破1000亿元。现阶段,我国信息安全行业下游企业主要有中国金融电子化公司、天和防务、国脉科技等。

作为信息安全产业的链长,国安信息在带动上下游企业共同发展上秉持两个方针:共建、共享。共建,即技术共建,国安信息会邀请不同领域的技术团队共同开发,各自发挥不同领域的技术优势,从而实现真正意义上的技术共建。共享,即市场共享,技术既然是共建的,那么成果一定要共享。国安信息在全国建设了30多个办事处,具备较强的市场拓展能力。国安信息从行业内筛选优质的信息安全类产品,通过自己的渠道进行推广,让更多的企业都进入到信息安全的大生态圈,共享信息安全发展的红利。

专家观点

邬贺铨:网络安全需打通产业链共享情报

近日,ISC名誉主席、中国工程院院士、中国互联网协会咨询委员会主任邬贺铨在第九届互联网安全大会上表示,网络安全需要打通产业链上下游共享情报,建立协同联动的联防联控机制。

当前互联网已经广泛渗透到我国经济社会的方方面面,在改进工作效率提升生活质量的同时,也增加了人们对于网络的依赖,从网络安全看,关系国计民生的关键是网络安全问题突出,勒索病毒攻击,新型网络诈骗,信息泄露,违法犯罪活动大量发生,基于此,邬贺铨分享了三点体会。

一是提升网络安全意识,加强国家安全数据安全、用户隐私保护。互联网企业通常都是大数据企业,基于大量的用户数据和所服务的企业数据开展业务。这些数据不仅包含了用户隐私,也有国家敏感的数据。但一些企业自律能力、对用户的敬畏和数据保护方面做得不够,给国家安全和数据安全带来巨大的风险,互联网治理的重要方面是规范数据的使用和安全保护,为整个互联网营造更好的发展生态,作为互联网企业,在发展中一定要加强国家安全、数据安全、网民利益和隐私保护的意识。

二是网络安全需要打通产业链上下游共享情报,建立协同联动的联防联控机制。随着数字化建设逐步加快,万物互联时代的到来,数据将由信息孤岛向共享高效利用发展,使得生产更高效和便利。但也带来一定的风险,在这种情况下,依靠单个企业的防御能力已不足以应对,需要在关联企业间形成威胁网络安全情报共享,制定威胁情报共享的标准,尤其是安全数据的输出和威胁情报的查询共享问题,建立协同联防的有效机制是非常重要的。

三是坚持产业创新和治理,进一步促进新创产业健康发展。首先要推动政府和相关机构,为新创企业打造量身的发展生态,进一步拓展市场和适用场景。其次要提高新创产品的质量,以发展的眼光对采购的产品和新创企业提出不断演进的要求,推动相关产品从可用到好用,进一步优化服务质量,完善产业体系。再次是提升新创产品的性价比,推动在关键领域落地的同时,也要加速向大众消费市场推广,为新创产品在更大的市场经受考验提供助力。

邬贺铨指出,未来互联网的发展应该是信息化和安全三轮驱动,兼顾发展和安全,将成为中国互联网持续发展的重要课题。

(本版稿件均由本报记者郭志明采访整理)