东软NetEye走自己的路

◎《商业伙伴》 张戈

东软NetEye是厂商，还是集成商？这并不重要。

在众多安全厂商中，东软NetEye的位置相当特殊。背靠东软集团，使方案商对与其合作总有顾忌，但优势也同样在此，东软NetEye对行业的理解，提供整体解决方案的能力，也是其他安全厂商所不能及。

走自己的路

特殊的背景，决定东软NetEye必须走一条自己的路。东软网络安全产品营销中心总经理赵鑫龙说："已经不可能靠一个厂商的几个产品就解决客户安全问题，用户需要的是集合多厂商产品的整体解决方案，以及专业的集成、运维和服务。东软NetEye希望在未来的5~10年成为客户在安全方面的一站式合作伙伴。"

从赵鑫龙的态度中不难发现，东软NetEye的定位似乎在发生变化，其更像是一家有自有品牌产品的安全方案商。对此，赵鑫龙并没有完全予以否认，"面对中高端客户，东软NetEye定位为安全方案商，在中小企业客户市场，东软NetEye正在推出定制产品，并渠道合作伙伴模式，覆盖3~4级市场。"

目前，东软NetEye的策略是，靠整合集团各事业部应用加强"内销"，"外销"则靠渠道。如此定位其实也不难理解，安全厂商的生存状态确实不容乐观，各品牌间同质化产品竞争头破血流，利润下降，导致研发投入降低，进而是产品更新换代速度减缓，恶性循环使既有产品价格战进一步升级。"安全厂商已经面临生存问题，东软NetEye希望新模式跳出恶性竞争的怪圈。我不在乎别人看我是厂商，还是集成商，东软集团顶级方案商的地位，也注定东软NetEye不可能采用与其他安全厂商一样的销售模型。" 赵鑫龙说，"在所有安全厂商中，只有东软NetEye既懂安全，又懂行业应用。我们希望与东软集团其他行业事业部继续加深合作。例如，与金融事业部的合作，东软NetEye可以为用户提供代码级的安全方案，目前，只有东软NetEye能做到。"

模式创新

战略定位已经确定，战术打法也正在更新。目前，东软NetEye确定了云计算、物联网、工业控制、移动互联为四大发展方向，其中云计算战术已经初步形成，东软NetEye将为用户提供云安全和安全云两种服务模式。

首先来看云安全，即为云数据中心提供整体安全解决方案。其实，东软NetEye的产品线已经相当齐全，2012年初，推出9款产品，使其几乎覆盖了从网络层到应用层所有的客户安全应用，但赵鑫龙表示，"到目前为止，我没看见哪家厂商的产品能满足云数据中心的所有安全诉求。东软NetEye安全定位为有整体集成、服务能力的安全方案商。" 与其他厂商合作，是必然的选择，而对于合作模式，赵鑫龙认为，"靠传统系统集成模式，不能适应云计算环境下，数据中心体系和架构上的变化，安全厂商之间需建立以技术合作为基础的模式，创新沟通机制和部署方法"。

同时，东软NetEye还创新地推出了"安全云"，如果说，在推进云安全时，东软NetEye的角色定位是方案商，面向"安全云"时，东软NetEye则服务商。

东软NetEye以B2B或B2B2C两种模式向用户提供安全服务，也就是说，用户可以直接购买东软NetEye云安全平台的服务，东软NetEye也可以与第三方合作，双方进行利润分成，联合提供服务。

东软NetEye "安全云" 模式在国内尚属首例，其工作原理是，通过"安全云"，管理用户海量日志信息，以大数据分析发现日志中潜在风险，进行预判。赵鑫龙认为，"东软集团在强调创新，但创新不能凭空臆造。在安全领域，商业模式创新，比技术创新更急迫。未来，东软NetEye更多地会以销售服务的模式，推进公司发展。"

创新时代下的金融信息安全之道

—东软NetEye出席2012金融业CIO圆桌论坛

近期，由中国信息主管网主办的2012年金融业CIO圆桌论坛在北京举行，东软网络安全营销中心安全服务部技术顾问胡甜，咨询方案部技术顾问李仰耀、何欣阳参加了此次论坛。论坛中针对银行证券业如何有效化解云计算和虚拟化之路的安全隐患等热点问题进行了讨论，东软安全服务部顾问胡甜认为从安全的角度考虑，不能把所有鸡蛋放在一个篮子里，但是云的概念是把我们所有的数据都统一，要做大集中，所以就要做好标签，大家好共享。在如何看待大数据应用，如何有效防范信息风险的话题讨论中，东软网络安全营销中心咨询方案部技术顾问李仰耀谈到，我们对云安全的担忧，更多地来自将应用、服务推向云端，交由云服务提供商来管理后的不可控性。目前东软安全提供的与云计算有关的解决方案包括两部分：一是东软能够提供涉及云环境、虚拟环境的内控和防护；二是能够为用户提供基于云的、针对服务器、网络设备的在线安全监测服务。

通过与行业用户频繁、深入的交流互动，了解用户最新的应用需求，并结合当下威胁动态，东软NetEye以专业的技术和丰富的实践经验，为广大行业用户提供务实、高效的信息安全整体解决方案。

现场合影

会议现场

东软NetEye渠道招募会在韶关、珠海两地顺利召开

近期，东软NetEye渠道招募会韶关、珠海两站在当地五星级酒店顺利落幕。相关市政府领导以及当地多家知名渠道代理商合作伙伴参加了会议。

会议中，广州凌创公司总经理郭志武先生作为东软多年合作伙伴代表，同到会者分享了与东软安全合作期间的经验和体会。随后，东软华南区技术总监那奇志讲解了东软最新的信息安全解决方案。东软安全广东区域渠道经理王景保为到场合作伙伴介绍了东软安全渠道策略以及等级保护项目运作和相关政策。期间，对于合作伙伴们提出了问题东软公司代表都予以详细解答。

通过此次会议，东软安全加强了与韶关、珠海区域渠道合作伙伴的沟通，加深了合作伙伴对东软公司及NetEye信息安全产品的了解，增强了双方的合作信心。很多渠道合作伙伴表示，希望东软能提供更多的技术培训机会，更多有技术前瞻性、需求量广泛的产品线以及行业合作案例、成功经验等。相信，通过不断总结经验，加强合作与支持，未来东软安全与渠道合作伙伴的关系将更加紧密，彼此的合作将更加顺畅，更加富有成效。

韶关会议现场

珠海会议现场

东软NetEye出席第五届中国信息主管年会医疗分论坛

2012年11月15日，由中国信息主管网主办的第五届中国信息主管年会医疗分论坛在北京国宾酒店成功举办，相关政府领导、行业专家、业内咨询顾问、IT知名企业代表参加了会议。东软网络安全营销中心咨询方案部部长徐松泉代表东软安全出席了会议并做题为"以HIS为核心的医院等保建设"的精彩演讲。

徐松泉在演讲中提出，东软面向各级医院为中国医疗卫生行业的信息化建设提供全面的安全解决方案。响应卫生部关于医院等保建设的要求，东软在等保建设的每一个领域和环节都有专业的团队为用户提供支持与服务，结合其在信息安全和等保领域的经验与技术积累，东软为医疗行业用户提供符合等保标准，将人、技术及流程有机结合，让安全技术和产品发挥更大效用的信息安全保障体系建设咨询与服务。

会议现场

月刊

2013年 1月出版

东软安全报

http://neteye.neusoft.com | 咨询热线：400-655-6789

NetEye 1996 因需而变 因御而安

◎ 总经理新年寄语

携手发展 持续共赢

2013年我们欣喜地迎来了东软集团旗下核心产品线——东软NetEye安全品牌17岁的花季之年。回顾我们安全产品17年发展之路，在各界领导及合作伙伴的支持帮助下，我们风雨兼程，一直坚持着对事业的梦想和追求。

我们用17年积累的安全经验提炼对用户产生持久影响的安全理念；我们用17年积淀的安全技术为用户提供务实可靠的安全保障服务；我们用17年积攒的安全行业整体解决方案能力为用户的信息化业务保驾护航。作为中国信息安全产业界的知名老品牌，我们感谢各行业用户及合作伙伴17年来对我们的支持与帮助、认可与理解。2013年，东软安全将继续秉承我们的宗旨，帮助客户创造更多的价值，只有客户价值得到提升，才能保持双方稳定而长期的合作。

东软NetEye坚持以成为中国最优秀的信息安全整体解决方案供应商为目标，坚持不断创新、不断发展的经营理念，坚持为我们的客户及合作伙伴不断地创造价值，不断地提供务实、可靠、优秀的产品，以提供对用户业务深刻理解、精湛卓越的信息安全整体解决方案为己任。

2013年我们期待能与大家携手发展，持续共赢！

东软网络安全产品营销中心总经理 赵鑫龙

2013年1月

东软发布移动设备安全管理系统

[2012年11月22日，中国·北京] 近日，东软在北京正式发布Cumquat移动设备安全管理系统。这是东软在网络安全领域，针对越来越多客户的移动化办公趋势和需求变化，融合多领域技术积淀，在国内率先研发推出的全新产品。该系统能够有效解决客户在移动化部署过程中面临的移动终端策略、安全、管理和应用等方面的问题，为各行业客户的移动化战略部署提供安全、敏捷的移动办公空间。

东软Cumquat移动设备安全管理系统由客户端和管理员端两部分组成，采用基于OMA设备管理（DM）标准协议设计开发，并将全部管理服务部署在云服务器上实现。管理端采用Web Application的开发模式，管理员通过浏览器登录服务器地址即可注册管理帐号，并通过网络对受管理移动设备进行远程管理。客户端在MDM企业应用商店下载并安装东软MDM终端应用后，登录管理员分配的帐号加入管理，同时客户端与管理员端通过Wi-Fi/3G网络进行通信。

随着移动化浪潮席卷全球，越来越多的人摆脱办公室的枷锁，通过智能手机等移动终端来处理日常事务。员工自带设备进入企业应用引领的移动办公新模式是未来发展的重要趋势。人们利用智能移动设备，通过正在加速发展的WiFi、3G、4G等新一代移动网络技术，使用高效率的办公应用软件，与办公网络便捷、无缝连接，将繁琐的工作融入科技的便利中，但对于企业来说，机密数据的安全性、办公行为的不可控等因素也给移动办公带来了很多隐患。

面对上述的诸多挑战，移动设备安全管理产品应运而生。它不仅能使IT部门更有效地控制和管理员工的移动设备群，并能保障移动设备本身及其信息数据的安全，从而帮助企业提升生产效率、竞争力和服务能力。

东软Cumquat移动设备安全管理系统针对终端设备，在特殊情况下支持安全锁屏功能，防止信息被盗；可以实时监控移动终端，一旦发现越狱或root化设备，能够警示管理员尽快采取相应的措施及时保护机密数据安全，如远程锁屏、植入新密码、发送警告信息、擦除设备重要数据等；当移动设备暂时无法找到或者丢失，管理员可以在东软Cumquat移动设备安全管理系统服务器端查看到设备的当前位置及其之前的运行轨迹；若移动设备丢失后无法找回，可远程擦除终端上的数据；东软Cumquat移动设备安全管理系统应用商店提供了一个集中的管理空间，管理员能够集中管理企业的应用程序，针对每个设备定制化的进行远程分发；该系统还支持分级推送策略，即在整个管理系统内根据不同用户角色、不同设备类型的群组划分，推送不同的安全管理策略，以确保为不同级别用户的设备提供有针对性的安全保护。

现场讲解

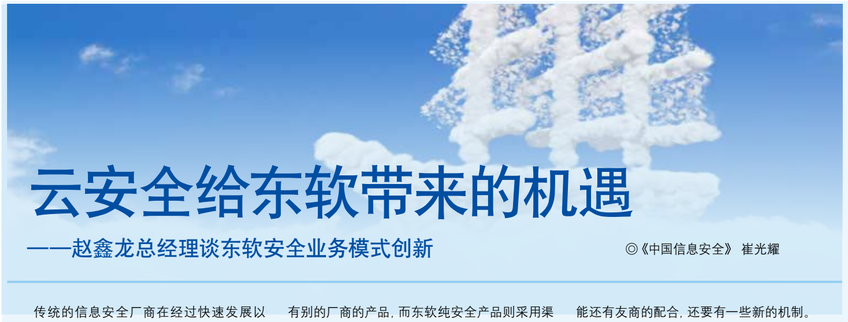
演示环节

东软NetEye出席"云计算与信息保密"学术研讨会

2012年12月1日，由中国计算机学会信息保密专业委员会举办的"云计算与信息保密"学术研讨会在北京召开。会议以研究云计算环境下信息安全保密问题，做好新形势下涉密网络安全保密管理和科研工作为主题。会议联合行政管理部门、学术机构和产业界的专业人士，针对普遍关注的云计算环境下的安全保密需求、终端和数据保护、安全框架以及测评技术等问题，共同研究探讨了云计算安全保密面临的机遇和挑战。

会议由中国科学院信息工程研究所所长孙德刚主持，国家保密局副局长戴应军，信息保密专委会主任杜虹致辞。东软公司网络安全产品营销中心总经理赵鑫龙出席学术研讨会，并作为特邀报告人做题为"云计算安全保密的实践"的主题演讲，报告针对云计算的安全挑战，云计算安全体系进行剖析，重点分享了东软云安全策略、集成云安全解决方案。在自由讨论环节中，参会领导和专家多次提及东软安全产品及解决方案，并希望东软秉承与时俱进，紧跟用户需求，打造安全产品及解决方案的良好传统，再接再厉，为我国信息安全保密管理及科研工作贡献出按需定制的整体解决方案。

东软网络安全营销中心总经理赵鑫龙做现场精彩报告



云安全给东软带来的机遇

——赵鑫龙总经理谈东软安全业务模式创新

◎《中国信息安全》 崔光耀

传统的信息安全厂商在经过快速发展以后，眼下大都面临着如何扩大业务，提升发展空间的困惑，在沉寂中寻求发展的方向。

在10月19日“东软解决方案论坛2012”大会上，东软集团董事长兼CEO刘积仁博士作了题为《变革时代的创新》的主旨演讲，着重强调东软正在力推的商业模式创新，这一战略同样体现在东软网络安全领域。东软网络安全产品营销中心总经理赵鑫龙在南昌接受采访时阐述了东软安全业务模式创新的举措，给出了一条积极的探索路径。

重新定位找准目标

东软从纯粹的安全产品提供商向整体解决方案提供商转换始于去年，原因在于这一角色转变和新定位，最能体现东软在应用解决方案方面的综合能力和优势。从外部因素看，安全发展到今天，已不再是一个厂商或者是几个产品就能解决客户的安全问题，因而组合一些厂商或者安全设备，包括为客户提供综合规划、设计、集成、维护、支持、服务等，才能够真满足客户的需求。东软明确，将在未来五到十年，朝着这个目标发展。这样一来东软安全业务就细分为两个部分：对于中高端客户，以整体的解决方案为主，其中有东软的产品，也可以有别的厂商的产品，而东软纯安全产品则采用渠道的方式去推销。一方面抓住一些大型客户，另一方面大力发展渠道，而且要覆盖到二三线城市。

赵鑫龙表示，过去东软一直在中间徘徊，这么多年来走下来，我们认识到必须有新定位才能有大的发展。在业务发展方向确定下来以后，再规划未来的整体发展策略，针对云计算潮流我们提出了安全云战略，提供整套的安全方案，就是我们基于云计算的平台，然后提供安全监测服务，这是另外一种新的商业模式。未来我们还会在物联网、工业控制、终端这些方面提出我们的发展战略。所以说东软应该是定位为一个大的集成方案提供商。

让云安全落地

东软的云安全策略是其业务转型的一个重点。据赵鑫龙介绍，云安全现在就是说我们能够给客户提供的，实际上是建设云数据中心的建设方案，包括其中的安全整体方案。在这方面，由于东软集团已经自己建了云数据中心，本身就是有建设的经验，包括运维的经验，做起来就省钱省事，具有较大的优势。当然这并不是说针对这个云数据中心的所有安全问题都能解决掉，但东软在朝着这个方向努力，它包括一些产品，可能还有友商的配合，还要有一些新的机制。

赵鑫龙谈到，东软已经在为北京市政府一百多个部门进行这方面的合作，提供海量数据的处理、采集、监测，初步实现了一些模型，得到的效果已经很不错了。由于属于战略性投入，先期研发把投入很大，目前看经济效益并不是主要的，但它的主要收获是东软在安全云方面的开拓，这种商业模式一定会给东软带来可观收益。由于这是一个蓝海，没有人跟你竞争，所以做起来基本上就没跑的。我们发展的客户越多，我们管理监测的网站越多，我们后端的处理能力会越强，我们的经验就会积累得越丰富，包括针对各种模型的升级、算法的升级都会越好，我们的服务也会越好。另一方面，我们与集团的业务天然联系，相互协作和促进，形成一套既有安全又有业务的解决方案，对客户就具有竞争力优势，未来东软将会进一步加深这种挖掘开发，在行业里面把我们的产品业务拉动起来，依靠这部分行业的补充，我们能够非常健康地活下去，而不是走同质化竞争的老路。

东软的探索让沉闷的产业界看到了希望。赵鑫龙说，东软一定要抓住这下一波的机会，现在是帮大家探探路，但愿这种探路能够标新出彩。

东软安全参加第35期学科前沿讲习班

2012年12月22至24日，由中国计算机学会主办、国家网络信息安全技术研究所协办的中国计算机学会第35期“学科前沿讲习班”在中科院计算所成功举办。

东软网络安全产品营销中心副总经理曹鹏、解决方案部部长徐松泉、安全服务部部长席斐及安全服务工程师胡甜参加了本次会议。会议围绕新阶段网络安全对抗的现状与趋势分析、海量恶意代码的处理流程与体系演进、安全漏洞与木马的攻防对抗展望、信息安全技术发展、机遇和挑战等最新话题进行了热烈的讨论，并且会议特邀国家网络信息安全技术研究所研究员、学术主任杜跃进及其他四位具备丰富实践经验的从业者、拥有深厚理论积淀的研究者、长期从事相关工作的思想者，共同围绕新阶段网络安全对抗体现的高级持续性威胁（APT）进行了深入交流与探讨。

网络安全发展到今天，越来越体现出对抗的特色：从过去围绕恶意代码的隐藏与查杀，到后来基于信息网络环境的攻击与防护，再到现在非常有目标的甚至国家之间发起的高级网络空间安全对抗。信息技术本身的发展变化、人类对信息技术应用的深化变化、新型网络安全对抗的动机和手段，这些相互关联的新情况给网络安全工作不断带来新问题。东软NetEye通过参加本期学习班，与业界专家的共同分享了实践经验和最新思想，共同探讨了应对网络安全对抗，确保网络安全的未来之路，东软NetEye将继续凭借17年的技术经验积累，为广大行业用户提供更先进可靠的产品和更贴近用户实际应用的安全整体解决方案。

会议现场

本土信息安全已穿上“盔甲”

稿件来自《中国科学报》 ◎ 作者：东软网络安全产品营销中心产品总监 王军民

话题背景

国家互联网应急中心最近的一份抽样监测数据，引发了业界对于中国信息安全的热烈讨论。根据该数据，2011年有近5万个境外IP地址作为木马或僵尸网络控制服务器，参与控制了我国境内近890万台主机，其中有超过99.4%的被控主机，源头在美国。而仿冒我国境内银行网站站点的IP也有将近四分之三来自美国。

有观点认为，中国的信息安全在以思科为代表的美国“八大金刚”（思科、IBM、谷歌、高通、英特尔、苹果、甲骨文、微软）面前形同虚设。而且在绝大多数核心领域，这八家企业都占据了庞大的市场份额。事情是否真的如此？

众所周知，信息安全是国家安全的重要组成部分。中国市场上最早从事信息安全的公司基本都诞生在20世纪末期，而美国从1967年就已开始研究计算机安全问题。从我国计算机发展历史来看，我国的计算机、互联网快速发展也是在20世纪末期，而当时美国已在计算机信息安全方面制定了健全的标准。由此可见，中国的信息安全发展起步落后显而易见。那么，这种落后是否意味着我国的网络是“赤裸裸”地摆在美国面前呢？

差距迅速缩小

如果说在上个世纪末，乃至本世纪初，我国的网络设备是美国“八大金刚”的天下，那么今天的中国已经在很大程度上摆脱了这种依赖。

由于政府部门高瞻远瞩，很早就已开始进行信息安全产业的培育，中国互联网方兴未艾之时即为我国信息安全兴起之始。今天的中国，网络安全厂商已经发展壮大成熟，网络安全方面也积累了诸多人才和大量的核心技术。

如今防火墙已经变得像交换机一样为人所熟知，政府、电信、金融等大型行业用户不再仅仅面向思科、Juniper等国外品牌进行采购。因为国内的产品已经足够成熟，所以选择高性价比的自家产品是最佳选择。而10年前的局面几乎是由思科、Netscreen（当时还未被Juniper收购）、Checkpoint等国际知名公司一统天下。

笔者欣喜地看到我国的网络安全技术总体上与美国正在逐步缩小差距，在相当大的范围内完全可以替代国外产品。我国已有自己研发的诸多安全产品，例如审计类产品、网闸、堡垒机等等都已经成为了在运营商、政府、金融等重要行业检测与防范入侵的重要设备，我们完全有能力构建一套国内自主的信息安全防御体系。

所以，从某种角度讲，虽然现有国内本土的信息安全防御没有达到“武装到牙齿”的地步，但至少可以说是穿上“盔甲”了。事实上也的确如此，在奥运、世博、大运会等等重要的活动中，通过使用国本土的主体技术、服务构建起了良好的防御体系，及时发现大量的、多种类的、来自国内外的攻击行为，没有让黑客攻击得逞，也没有出现重大安全纰漏。

缺乏安全方法论

事实上，即便是在美国这样的发达国家，信息安全防护也不是靠某种单一产品所能完成的。每一种安全技术单独的存在都是不健全的，体系化的安全防护才是最终的应对方法。

当前，我国已经有了自有品牌的交换机、路由器等网络设备，有了自主的防火墙、IDS等安全产品，但这些远远不够。它们彼此单独的存在就像一盘散沙，即便单体再优秀也无法达到良好的综合防护效果。万里长城的坚固关键不在于每块砖的坚硬，更重要的是这些砖有序地组合成铜墙铁壁。

反观发达国家的网络防护，所有的防护体系均不是单独靠产品罗列的，而是以充实的理论研究为基础，结合整体的信息安全解决方案所构成的。美国已经拥有数以百计与安全相关的各种法案、标准，这种深厚的积累需要持续积淀。而且，一套好的安全防护体系不能够防范所有攻击，攻与防的不断博弈导致在IT技术快速发展的今天，随时可能会发现新的漏洞。

正因为此，我们看到了著名的“维基解密”事件、看到了美国国防部网络屡次被入侵。无论美国“武装到牙齿”网络防护体系还是我国自有的防护体系，都需要悉心研究，做到有效防护、快速检测、快速反应、快速弥补的良性循环效果。客观地说，当前我国信息安全缺少的不是技术，而是如何让技术能够为用户真正实现体系化的、有效的信息安全防护体系的方法论。

在防患于未然之时，我们需要有一套规范的方法，指导企业构建自己的安全防护体系，科学地进行投资；而在攻击入侵之后，需要有快速的响应措施迅速清除攻击危害。

方法论是关键

回顾我国信息安全的发展历程，当前我们最缺乏的是如何形成一套完善的安全防护体系。

21世纪初期，我国曾大量采购防火墙、IDS等安全设备。经过多年建设后，大型的用户机房中总能看到很多防火墙、IDS彼此毫无关联地独立工作。难道管理员都无法了解自己所管理的网络中的安全状况？更可怕的是，大量的网络设备、安全设备充斥整个机房的大部分空间后，安全隐患已经不是一个普通网络管理员所能够应付的事情。所以，大量的用户开始有新的需要可视化、统一化的网络安全管理。

基于大量的用户需求，综合安全运维平台应运而生，在经历了几年的成熟期后已经能够为大型用户提供有效的安全事件关联分析、精确定位问题、安全形势趋势分析等更高层面的功能，解决用户信息化建设过程中遇到的信息孤岛问题。

如今，本土化的企业已经成功在海外市场“登陆”，国内知名的网络安全公司甚至已经将相关安全产品远销到发达国家，我国的信息安全技术已经向海外迈进了实质性的步伐。

笔者认为，这与我国安全技术在过去近20年间在技术、标准等方面的积累有关，也与这些企业自身建立的一套行之有效的方法论密不可分。国内的优秀信息安全企业凭借多年的技术积累和积极的标准研究，已经由点到面、由技术到制度等多个维度形成较为成熟的信息安全建设方法论。

今后，技术、标准、信息安全防护体系建设方法论将成为我国信息安全体系成功建设的关键因素。中国必将自力更生，构筑属于自己的信息安全“万里长城”！

东软Cumquat：给移动办公设备“上锁”

◎《中国计算机报》记者 高春燕

BYOD（Bring Your Own Device，自带设备办公）早已经不是什么新鲜事。Gartner预计，2012年智能手机销售量将达到6.45亿部，远超同期PC销售量。预计到2014年，有80%的商务人士将使用至少两台个人设备访问企业系统和数据 。IDC也认为，IT 消费化将是未来十年科技领域影响最大的趋势。BYOD、VDI（虚拟桌面）和 SaaS 正在改变企业端点模式：随着越来越多的企业数据和资源通过员工个人所有的、不受企业 IT 安全策略控制的移动设备来访问，安全违规或数据泄漏的威胁也大幅增长。

安全、管理双重考验

IDC 预测，随着移动化浪潮席卷全球，越来越多的人摆脱办公室的枷锁，通过智能手机等移动终端来处理日常事务。员工自带设备、安装和使用企业应用，引领的移动办公新模式是未来发展的重要趋势。人们利用智能移动设备，通过正在加速发展的WiFi、3G、4G等新一代移动网络技术，使用高效率的办公应用软件，与办公网络便捷、无缝连接，大幅提升了企业劳动效率。但与此同时，机密数据的安全性、移动设备的不可控等因素，也给移动办公带来了很多隐患。

东软网络安全产品策划部部长于江对移动信息化带来的安全问题感到担忧：“移动办公已经成为不可逆转的趋势。澳大利亚政府统一采购苹果的产品用于办公，并且统一部署安全策略。但在国内，苹果手机越狱之后，用户可以方便地从第三方应用商店下载应用程序，这导致苹果产品的安全机制失效。安卓的开放性更是导致黑客很容易获取安卓的源代码，加之安卓市场鱼龙混杂，充斥着大量盗版应用程序，根本没有安全性可言。”

移动信息化给企业带来了安全和管理两方面挑战。在安全方面，东软网络安全产品经理马志斌认为：“iOS硬件具有加密功能，iOS系统内部的安全机制能够部分解决安全问题，但是仍存在缺陷。安卓应用之间缺乏访问控制，带来的数据安全威胁严重。”在管理方面，移动信息化让企业IT变得更加复杂，部署时间长，缺乏有效的监管手段，设备功能难以限制。这些都让企业管理者头疼不已。

统一平台管理

近日，为应对移动信息化浪潮，东软集团发布了Cumquat移动设备安全管理系统。“2009年，为满足一个国外企业客户对BYOD产品的需求，东软开发了一套产品，就是Cumquat的雏形。”于江向记者介绍称，“Cumquat由客户端和管理员端两部分组成，能有效解决客户在移动化部署过程中的移动终端策略、安全、管理和应用等方面的问题，为用户的移动战略部署提供安全、敏捷的移动办公空间。”

BYOD的一个特点是个人应用和企业应用同时存在，个人数据和企业数据混杂在一起。为保障企业的核心数据不外泄，Cumquat采取了一系列安全措施，包括安全锁屏、安全告警、安全监控、离线安全管理等。在某些特定的场景下，管理员可以通过后台系统限制用户调用照相机、浏览器、截屏、摄像机等应用，甚至对设备进行锁屏处理。马志斌介绍说：“例如，当进入制造车间时，员工不允许带任何物品。Cumquat可远程控制设备在特定区域内，自动进入安全锁屏状态，移动终端无法使用，以防止企业敏感信息泄露。当员工离开特定环境之后，移动终端又会自动解锁。”在他看来，安全锁屏是Cumquat最实用的功能之一。

在管理方面，Cumquat支持管理员对应用程序的集中管理，并可针对每个设备进行定制化的远程策略分发。同时，该系统还支持分级推送策略，在整个管理系统内可根据不同用户角色、不同设备类型，有针对性地推送不同的安全管理策略，以确保不同权限用户的设备和访问的安全性。

尽管现在才正式发布Cumquat，但实际上去年东软就已经开始承接各类项目。“凭借东软对医疗、教育等行业的深入洞察，结合不同用户的需求，Cumquat支持定制化开发，可为行业用户提供适合企业现状及业务需求的移动设备安全管理产品。”马志斌告诉记者，“比如在移动营销的应用场景中，销售人员用iPad展示产品信息，为了防止竞争对手拥拷贝相关内容，Cumquat支持远程服务器播放，而不是将资料下载到本地。此外，管理员还可以将最新的产品资料通过后台系统统一分发到销售人员的移动终端，以便销售人员能随时随地查看。”

内网安全将聚焦数据防护

◎ 畅享网 孔维维

随着社交网络、移动终端的普及，云计算和虚拟化技术的落地应用，企业内网安全将会遭遇哪些新的问题和困惑？企业内网今日的安全策略能否适应飞速发展的网络变革？内网安全下一个聚焦点在哪里？

本世纪初期，互联网的大规模普及带动了企业的网络应用的蓬勃发展。许多企业通过搭建内部局域网实现企业的信息共享和统一管理。10年的时间里，伴随着网络病毒的快速传播，企业内部网络安全问题不断涌现，各类网络安全事件频发。随着社交网络、移动终端的普及，云计算和虚拟化技术的落地应用，企业内网安全将会遭遇哪些新的问题和困惑？企业内网今日的安全策略能否适应飞速发展的网络变革？内网安全下一个聚焦点在哪里？

数据资产保护从管理开始

企业局域网的普及给企业内部ERP，生成自动化等应用系统的安全实施活动带来了极大的便利，企业内外每一项数据，都是企业的数据资产。但是因为企业内网的防护手段往往用防火墙来做网络边界，一旦翻过防火墙，企业数据资产将面临破坏的风险。

记者在采访东软网络安全营销中心产品经理郑玮时，她提出了这样的担忧，“常规安全防御往往是网关级别、网络边界等方面的防御，相反，来自内部的安全威胁是众多安全管理人员普遍反映的问题。对于企业的内网IT应用系统、数据库、核心服务器等都要足够的重视，对于这类核心资产不仅要从技术角度进行管理和审计，也要从管理者的角度出发。”对使用系统的使用者进行管理，从这个角度讲，内网安全应该技术手段与管理制度相结合，二者缺一不可。

东软网络安全营销中心产品经理郑玮

目前企业的各种资料、数据八成以上都是以电子文档和数据的形式保存。这些信息包含了企业的核心数据，对可靠性、保密性要求很高，一旦发生数据泄漏，后果不堪设想。而每个企业的安全状况都有所不同。郑玮表示，“内网安全管理一定要结合本单位的实际情况，引起领导的重视，明确人、技术、管理的三方责任。”

内网安全要和管理制度和规范结合起来，才能达到真正意义上的安全。而内网安全绝不仅仅是技术手段的堆积，更不是安全管理员的责任，管理和技术相互依赖，管理意识的出现正是因为来自内网的安全威胁，而这些安全威胁是需要相应的技术手段来实现的。内网安全管理是一个系统工程，要使用多个手段多管齐下。

行为审计不是企业的唯一选择

内网安全发展至今已经进入全面发展的成熟时期。针对不同类型威胁的内网安全产品也陆续推出不同的安全产品，有单个功能产品，也有整体的解决方案，范围涉及资产管理、设备加密、行为审计，数据防泄漏、透明加密等多个环节。

然而对于这些内网安全产品，企业员工却颇有微词。企业担心员工登陆不安全网站威胁内网安全，员工对企业的行为审计甚为反感，对此，郑玮在介绍采访时介绍说，“从最终用户的角度来看，为了提高员工IT操作的安全性和工作效率，部署行为审计类产品无可厚非，这也是合规的。从技术角度来看，行为审计并不一定侵犯个人隐私，比如说东软的行为审计只需要提供一些审计关键字，通过行为审计的方式，严格限制被审计人员对原始数据的接触，就能比较好地做到尊重个人隐私。”

市场上没有百分百完美的产品，行为审计也不是企业的唯一选择，目前供应商也开始转型，不但提供内网安全设备，还为用户提供咨询服务。“其实，现在安全产品供应商从设备提供商过渡到解决方案提供商，没有哪一家厂商可以说自己的产品包罗万象，可以满足用户的所有需求。用户目前更关注的是解决方案，其次才是实施的产品。”郑玮说到，没有方案就没有产品。用户在产品选择时也要更多地关注产品供应商的解决方案是不是符合自身的需求。

未来内网安全焦点在数据防护

云计算、移动应用、社交网络已经成为许多员工的日常应用，也成为内网的安全的绊脚石，用户在选择、实施内网安全技术和产品的时候，需要根据新的情况提出新的要求。企业内网今日的安全策略很难适应飞速发展的网络变革。郑玮说到，“未来内网安全防护的焦点将集中在数据防护，企业应该通过边界控制、身份认证、访问控制、移动介质管理、网络接入控制、审计与监控等各种安全技术手段从应用、管理和网络等各个方面共同保障数据安全。”

对于企业用户自身来讲，除了依靠供应商的安全方案外，本身需要对一些网络资源和安全隐患进行即时的发现和处理。用户大多需要大而全的方案，这也是其自身的实际情况决定的；也有些中小型用户的需求较单一，一般需要功能稳定的单一产品即可。不过不管是部署大而全的方案，还是单一稳定的安全产品，内网安全并不神秘难以把握。只有做到控制机密不被拿走，即使拿走也无法打开加密文件，从这个角度来看，企业内网安全已经步入数据防护的时代。