携手发展、持续共赢

——东软NetEye 2013年度渠道合作伙伴大会在珠海成功召开

2013年1月17日-19日，东软NetEye 2013年度渠道合作伙伴大会在珠海德翰大酒店隆重召开。会议的主题是携手发展，持续共赢，来自全国的近三十家渠道合作伙伴参加了此次会议。

会议由东软网络安全产品营销中心总经理赵鑫龙代表东软安全致词，赵总首先对到场的渠道合作伙伴表示欢迎，强调东软安全将在2013年给予渠道合作伙伴更大力度的支持，加深与渠道合作伙伴的合作共赢。东软网络安全产品营销中心副总经理巴连标则着重介绍了东软NetEye 2013年渠道策略。另外，在会议中还听到了来自渠道合作伙伴的声音，广州凌创信息科技发展有限公司和合肥东联信息科技有限公司的代表分别分享了他们与东软安全多年的合作经验。

许多合作伙伴在会后表示，通过本次渠道大会，更加认可东软NetEye的产品技术及公司实力，东软安全2013年的渠道政策很给力也令他们很感兴趣，更表达了坚定地同东软安全长期、稳定合作的信心。同时，合作伙伴们希望东软安全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分享更多的行业资源和成功案例。相信，未来东软安全与渠道合作伙伴的共赢发展会取得更大的成绩。

东软安全出席信息安全企业科技创新及需求研讨会

2013年1月16日，由科技部高技术中心、国家863信息安全主题专家组、公安部第三研究所、北京邮电大学联合举办的信息安全企业科技创新及需求研讨会在北京召开。会议主要探讨在大数据、移动互联、物联网等新的应用背景下信息安全企业面临的机遇和挑战，以及现阶段企业科技创新的思路和需求。

东软网络安全产品营销中心副总经理曹鹏和副总经理路娜出席了会议。曹鹏在会议中针对会议主题“大数据、云计算和SDN软件定义网络”做出了演讲。曹鹏指出，大数据是典型的价值低密度数据，采用传统的加密这样的防护手段并不适用于大数据。大数据更多的应该是被充分利用加速当前网络安全产品尤其是日志审计SOC类产品的研发，而当前日志审计类产品在做复杂的日志分析的时候依托传统的结构化数据库很容易遭受到性能瓶颈，而引入大数据这样的分析模式可以很好的加速产品的功能性能提升，如果国家能够在安全管理产品领域和大数据分析平台的研发工作中加大投入和力度将会起到很好的推动作用。另外，针对云计算话题，曹鹏谈到，当前行业内缺少针对云计算的安全建设指引，希望能够投入在这个领域出一个合理合适的标准。云计算中网络虚拟化传统的依托网络进行防护的安全设备面临淘汰，如何针对虚拟化积极升级改造目前的安全设备，这方面目前国外已经有了很多成功的先例，但是我们国内相对而言还是比较落后的。曹鹏表示，未来的网络是扁平化的，网络设备与转发控制将分离，随着SDN技术和OPENFLOW协议的普及，对现在的传统网络架构冲击会非常大，如何建设符合SDN标准的网络安全方案和研发符合SDN规范的网络安全设备，也应该是国家进行重点扶持的一个技术领域。

面对当今信息安全面临的机遇和挑战，东软安全将继续努力实现信息安全领域的科技创新，加速产品研发，提升产品性能，更好地满足行业用户的信息安全防护需求。

会议现场

东软云安全产品亮相国家“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。

珠海会议现场

东软被评为2012年度海南省CIO可信赖的信息安全服务商


会议现场

2013年1月18日，海南省信息安全大会于在海口市隆重召开，会议搭建了各行各业信息安全主管与产业界领导、专家、厂商交流的平台，也是信息安全企业的最新信息安全技术及产品展示的大舞台。来自海南省各个行业从事信息化和信息安全工作的主管领导，技术骨干及国内行业代表100余人出席大会。会场同时设立产品展示区，供省内外参会企业展示新产品、新技术、新成果。

东软作为2012年海南省CIO可信赖的信息安全服务商应邀出席了本次会议。东软网络安全华南咨询顾问李昕做了主题演讲，重点阐述了东软公司在网络安全领域中的技术优势和产品技术特点。

海南省高度重视信息化建设，“十二五”期间将计划启动一系列重大信息化工程专项建设，打造“信息智能岛”，东软将参与海南的信息化建设，为提高海南省信息安全保障能力，为信息智能岛和国际旅游岛信息安全建设保驾护航。

东软NetEye荣获2012年度“中国 IT 商业伙伴冠军”称号

2013年1月16日，2012商业伙伴冠军论坛暨商业伙伴大学成立典礼在北京隆重举办。会议中，东软安全获得2012中国IT商业伙伴冠军调查评选信息安全类产品备件储备满意度第一名的好成绩，东软安全的渠道支持体系和支持力度得到了合作伙伴们的高度评价。

颁奖现场

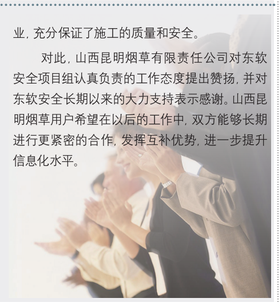
商业伙伴冠军调查，是由商业伙伴咨询机构针对渠道合作伙伴对于IT厂商渠道支持满意度的全面评估。该调查源自开展了近10年的中国IT渠道冠军调查评选活动，采用渠道合作伙伴为产品品牌打分的方式，涉及销售支持，营销支持，服务支持三大类15个细分指标，整体得分第一的品牌获得商业伙伴冠军称号。自2012年9月启动以来，调查历时近3个月，获得了约5000个有效样本。此次获得“中国IT商业伙伴冠军”称号，东软安全以技术实力和完善的渠道体系政策再次获得了合作伙伴的认可 。

东软安全喜获山西昆明烟草用户表扬信

近期，东软安全收到来自山西昆明烟草有限责任公司的一封热情洋溢的表扬信，对东软安全项目组成员在山西昆明烟草网络系统改造项目中表现出的专业技术、敬业精神予以赞扬。

在该项目实施过程中，东软安全现场实施人员对施工质量，工艺严格把关，团结协作，认真负责，充分发扬不怕苦不怕累的作风，精心组织安排项目每项施工内容，在有线与无线网络技术方案、技术规范等方面做了大量工作，体现了很高的技术素养，敬业精神以及优质的服务意识，对于施工工程中最困难的设备搬迁工作，施工人员不分昼夜加班加点，在计划时间内圆满完成了任务，东软安全项目组成员对待工作认认真真，兢兢业业，充分保证了施工的质量和安全。

对此，山西昆明烟草有限责任公司对东软安全项目组认真负责的工作态度提出赞扬，并对东软安全长期以来的大力支持表示感谢。山西昆明烟草用户希望在以后的工作中，双方能够长期进行更紧密的合作，发挥互补优势，进一步提升信息化水平。



3 月刊

2013年3月出版

东软安全报

东软NetEye

您身边可信赖的信息安全整体解决方案提供商

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

东软发布安全云

2013年1月21日，东软在北京正式发布东软安全云。该平台基于东软Aclome敏捷云应用管理平台，可以灵活部署在不同品牌的虚拟化云环境中，是传统安全服务与SaaS云监测相结合的一站式全新在线服务平台。东软安全云能够为用户的网站、服务器及网络安全设备提供在线安全监测服务，帮助用户显著降低安全监测管理的实施成本，提升运维团队的工作绩效。通过遍布全国、日益增多的东软云服务监测节点，收集、分析大量一手的监测告警数据，丰富网络安全监测服务的总体信息量，从而使用户更准确地把握和感知整体安全态势。

据介绍，东软安全云通过“线上与线下”结合、“软件与硬件”结合的模式，为政府、金融、企业、能源、电信、电力、航空、医疗、传媒、教育等大型行业网络及中小企业用户提供安全监测、咨询、维护及整改等综合服务。

“线上与线下”

通过东软安全云，在线为用户提供各类SaaS云监测服务。东软专业安全服务团队根据用户实际需求，能够提供远程或驻厂的综合安全服务，解决用户网络中存在的各类安全问题；而线下服务则以信息安全应急响应服务为主。

“软件与硬件”

东软安全云为用户提供的是SaaS服务，即软件监测服务。但当用户有需求时，东软同样能在硬件安全设备方面给予支持，并且对于购买一定年限SaaS服务的用户，东软将免费提供硬件安全产品及服务。根据服务内容和形式不同，东软推出不同层次的收费标准，全面提升网络整体的安全性、稳定性和可靠性。

东软云监测服务替代传统安全监测的主要优势

首先，可以提高用户信息系统的整体安全性，减少用户在建设安全监测平台时所产生的巨额投资。通过东软安全云进行统一的事件研判分析和专业应急处置服务，提高用户自身安全运维人员的工作绩效，提升安全监测运维工作标准化和质量。

其次，东软安全云监测服务功能采用开放式模块设计理念。面对用户不同的要求，可以快速集成更多产品并转型为SaaS服务模式，为用户提供更便捷、丰富的服务。

东软安全云充分考虑到面向未来服务用户可能出现的更多信息安全监测防护技术需求，通过开放的支撑功能模块化架构，不断自身升级、完善。对于服务用户而言，所有监测服务功能升级都不需要重新部署系统，或者增加任何额外的软硬件基础投资，只需访问东软安全云网站，轻松选择所需新增服务，即可享受云服务升级所带来的全新体验。

据悉，东软安全云已经通过工业和信息化部软件与集成电路促进中心（CSIP）“基于安全可控软硬件产品云计算解决方案”的专家评审，并已经在多家商业银行、IDC数据中心以及大型央企用户中得到成功应用。依托在安全产品技术研发领域17年的积累，东软积极推进中国云安全服务标准化进程，推动安全服务传统产品形态向服务形态转变。未来，东软将继续面向行业和企业用户，提供更加智能、先进的B2B、B2C的云安全服务，实现东软在信息安全领域中为用户提供更多的面向云服务、云安全更具创新性、应用性的增值服务。



发布会现场

东软安全签约秦云工程 助力我国西部首个云计算服务应用示范平台建设

[2013年2月1日，中国•西安] 2013年2月1日，由中国电子西安产业园发展有限公司联合西安市经开区管委会主办的“秦云之业”展示答谢会隆重启幕，。在本次晚会上，由东软安全联手中国电子西安产业园开发建设的“秦云”工程首度亮相，获得了到场嘉宾的高度认可。

2012年8月，中国电子西安产业园在国家部委和省市区各级政府的大力支持下正式启动“秦云工程”，加快发展以云计算服务产业为代表的战略新兴产业，以应用促发展，进一步落实“统筹科技资源，促进科技成果转化”，打造中国电子西安产业园云计算服务特色产业基地和建设云计算服务应用示范平台。

目前，“秦云工程”项目进展顺利，其整体规划包括云计算服务专业园区和云服务应用示范平台两个部分。其中云服务应用示范平台已于2012年12月投入试运行，首期重点推广六项云服务，包括云存储、云桌面、云财税、云办公、云座席和云安全等。在众多提供云安全服务的厂商中，最终中国电子西安产业园与东软安全达成战略合作，共同建立我国中西部安全云运营管理中心，双方也将对中西部安全云产业市场，包括中西部政府、金融、大型企业、SMB行业云市场的开拓和产业链整合等进行深入的合作。

东软安全云是基于东软Aclome敏捷云应用管理环境之上的一站式SaaS云服务平台，能够为用户的网站、服务器及网络安全设备提供在线安全监测服务。同时，东软安全云通过“线上与线下”结合、“软件与硬件”结合，为用户提供安全监测、咨询、维护及整改等综合服务。


东软安全云展厅现场交流

针对政府、军工、金融、能源、电信、电力、航空、医疗、传媒等行业大型网络用户以及中小企业用户，东软安全云为之所提供的在线信息安全监测服务，可以将传统安全服务模式与云监测技术相结合并进行创新，能够显著提升服务团队的工作绩效，积极推进云计算服务的标准化，扩大服务的受众面。同时，通过云监测服务收集和分析大量一手的监测告警数据，丰富了网络安全监测服务的总体信息量，帮助用户更准确地把握和感知整体安全态势。

2013年，东软安全将继续本着持续创新的精神，以高质量的技术和服务，助力加快“秦云工程”云服务应用示范平台和云计算服务产业园区建设，以中小企业服务应用为切入点，建立完善园区公共服务能力和服务体系建设，使中国电子西安产业园成为我国西北地区首家以云计算服务聚集和技术创新为主题的产业平台，努力协助中国电子西安产业园将“秦云工程”打造成为中国云计算服务产业的一面标志性旗帜。

经国家权威测评机构认证，东软NetEye打造国内首款功能完整的IPv6版UTM产品

近期，东软NetEye万兆集成安全网关NISG（IPv6版）顺利获得国家信息安全测评信息技术产品安全测评EAL3级证书，同时成功入选国家发改委下一代互联网信息安全专项UTM类产品测试名单。据了解，此次获得UTM类IPv6版EAL3认证证书的企业仅有两家，东软NetEye凭借17年的深厚技术实力和丰富的实践经验再次得到业内专家和用户的认可。

2012年，国家发改委决定组织实施国家下一代互联网信息安全专项工作，旨在重点支持满足下一代互联网发展需要的高性能网络信息安全产品。专项要求产品必须同时支持IPv4和IPv6环境，符合IPv6相关规范要求，能够满足IPv6环境下各种场景的网络信息安全需求。同时，产品自身应具有较高的安全性。

经过中国信息安全测评中心专业、细致、严格的测试评审，东软NetEye NISG产品通过了全部功能和性能测试，UTM功能支持IPv6环境的程度达到100%，成为国内首款功能完整的IPv6版UTM产品。

近年来，IPv6网络的普及速度很快，然而IPv6网络上的安全防护却存在着非常大的隐患。目前多数网络安全产品或者不支持IPv6，或者只支持路由、包过滤等简单功能，当用户在IPv4向IPv6网络切换时，网络安全水平就倒退到十年前的简单防火墙阶段。而此次通过测评的东软NetEye集成安全网关（NISG）产品，支持IPv6环境下几乎全部的UTM功能，包括支持IPv6下的协议识别、入侵防御、URL过滤、垃圾邮件防御、病毒防护等。

另外，东软NetEye NISG系列产品在高性能防火墙架构基础上，率先突破了UTM产品的应用层性能瓶颈，在使用协议识别功能的情况下单板吞吐能力可达到30Gbps以上，处于业内领先水平。

—— 医疗行业解决方案 ——

全国三甲医院等级保护项目解决方案

医疗卫生行业与人民身心健康和国家人口素质密切相关，医院信息系统建设也始终围绕更好地为人民提供医疗卫生服务展开。医院信息系统的安全性直接关系到医院医疗工作的正常运行，一旦网络瘫痪或数据丢失，将会给医院和病人带来巨大的灾难和难以弥补的损失。同时，医院信息系统涉及大量医院经营和患者医疗等私密信息，信息的泄露和传播将会给医院、社会和患者带来安全风险。

医疗卫生行业目前不仅面临着全新的信息安全挑战，而且还存在许多长期以来的安全问题，比如医院信息安全缺乏标准化管理，核心软硬件防护技术较为单一，数据中心防护能力不足。作为国内领先的信息安全整体解决方案提供商，东软始终秉承以客户为中心，致力于为客户打造安全、稳定、持续运行的医疗卫生信息化服务平台和系统。东软NetEye具备坚固的安全技术防御体系及完善的信息安全管理流程，助客户全面提升人员安全意识和安全技能，并配备专业的安全服务响应服务，有效应对人为因素，信息系统自身缺陷、外部因素带来的不利影响，充分保障医疗卫生行业客户的业务稳健发展和创新。

东软NetEye助力三甲医院等保建设的六大优势

优势一：对HIS系统的深入了解和经验积累

东软从1996年开始进行HIS研发，已有17年HIS系统研发经验，承担过众多三甲医院HIS系统开发工作，对HIS系统应用特点、运维流程、权限控制等各方面都有深入了解，可以根据业务安全保障需求设计出全面的HIS系统安全方案。

优势二：丰富的行业信息安全建设经验和成功案例

东软NetEye17年来为金融、电信、政府、医疗、能源、航空、企业等行业用户提供全面的信息安全解决方案，积累了丰富的项目实践经验，尤其是在卫生系统及三甲医院安全防护建设方面也有诸多成功案例。

优势三：最高级别资质认证和专业人才储备

由于HIS系统等保安全保障体系建设涉及到数据安全、应用安全、网络安全、链路安全、物理安全等各个层面，因此需要在各个领域，各个层面都要有专业的人才，才能够真正保证用户系统的高安全性和高可用性。东软具备计算机信息系统一级集成资质，反映了厂商整合不同系统、不同设备，保障业务系统安全和业务数据安全的专业能力。同时，东软还具备信息系统安全集成资质证书，在安全集成领域具备明显的领先优势。

优势四：性能卓越的安全防护产品及领先的、一体化的IT综合运维与安全管理平台

东软NetEye防火墙作为网络安全防护的中流砥柱，有众多的卫生系统和三甲医院部署成功案例。据权威第三方调研数据显示，自2001年以来，东软NetEye防火墙连续11年位居国内市场份额首位。东软防火墙产品的稳定和成熟度已充分经历了市场的考验，在金融、政府、医疗、电力、电信、教育、企业等各领域有10000家以上的成功案例。

东软IT综合运维与安全管理平台已经先后成功部署于北京市电子政务安全监控中心和环保部IT系统综合监控与运维中心，是目前国内先进的、部署规模较大的IT综合管理平台，功能涵盖网络管理、应用系统性能监控、安全事件统一审计与响应等。

优势五：优秀的本地化服务能力

东软NetEye在全国34个省会及主要城市均设有分支机构，提供本地7*24小时的技术保障和应急响应服务。同时在沈阳、大连、成都、南海、海南建设了五个大型培训基地，投资数千万，具备专业的应用、网络、安全培训实验环境，可以为各行业用户提供集中的知识技能培训。

东软大连培训基地　东软南海培训基地　东软成都培训基地　东软沈阳培训基地

另外，安全保障系统建设完成后，日常的运行和维护过程中，一旦出现安全事件，往往需要由厂商提供应急响应，因此要求厂商必须具备这方面的专业能力和权威认证。东软具备“信息安全服务一级应急处理服务资质认证”，一旦接到用户的应急响应请求，可以马上按照规范的流程为用户提供专业的应急响应服务，迅速、果断、高效地处理安全事件，降低或避免损失的发生。

优势六：AAA级信用资质

在选择安全保障体系建设合作伙伴时，信用资质也是应当重点考察的内容之一。东软具有AAA级信用资质，具有优秀的信用记录，企业文化稳健厚重，是卫生系统及三甲医院用户可信赖的合作伙伴。

成功案例分享

重庆开县人民医院

近期，东软安全成功签订重庆市开县人民医院等级保护信息安全建设项目，有效拉动西南地区各大三甲医院的等保工作的项目的全面开展起到了区域示范作用。东软NetEye高性能防火墙及上网行为管理系统（NIBC），应用于重庆市开县人民医院信息网络安全防护中，保障数据安全交互与传输。东软NetEye防火墙及上网行为管理系统凭借先进的技术、稳定可靠的运行性能，为重庆市开县人民医院的办公网络的互联网安全接入提供了全面的安全保障。

在长期与重庆市开县人民医院携手同行的过程中，东软不仅展现了优秀的集成解决方案的能力，而且还为客户提供专业的安全服务及国家级应急响应服务。当任何时刻用户网络信息系统出现安全危机事件时，东软都第一时间和客户站在一起，共同面对问题，及时解决问题。

上海中医药大学附属曙光医院

上海中医药大学附属曙光医院是一所沪上的百年老院，三级甲等综合性中医院，位列上海十大综合性医院之一、全国示范中医院。多次获得全国医院文化建设先进单位称号，2009年获得了国务院颁发的“上海市迎世博优质服务贡献奖”。2001年成为全国首家通过ISO9001质量管理体系认证的中医医院。2010年，上海市人民政府和卫生部将曙光医院列为省部共建研究型中医院。

根据上海市卫生局的要求，曙光医院HIS、LIS、RIS/PACS系统定级为等保三级系统。在医院的信息化建设过程中，应当正视可能面临的各种安全风险，对网络威胁给予充分的重视。为曙光医院信息网络的安全稳定运行，确保医院信息系统建设项目的顺利实施，东软NetEye结合具体的网络和应用系统情况，根据曙光医院目前的计算机信息网网络特点及安全需求，本着切合实际、保护投资、着眼未来的原则，提出等级保护信息安全集成方案，与曙光医院展开全面合作。

医疗卫生行业目前不仅面临着全新的信息安全挑战，而且还存在许多长期以来的安全问题，比如医院信息安全缺乏标准化管理，核心软硬件防护技术较为单一，数据中心防护能力不足。东软NetEye拥有坚固的安全技术防御体系及完善的信息安全管理流程，全面提升人员安全意识和安全技能，并配备专业的安全服务响应服务，有效应对人为因素，信息系统自身缺陷、外部因素带来的不利影响，充分保障医疗卫生系统业务稳健的发展和创新。

—— 政府行业解决方案 ——

国家财政部SOC项目解决方案

项目需求：

东软NetEye SOC集成了网络管理、安全管理和运维工单三部分功能。因财政部已经部署有单独网络管理和运维工单系统，因此本次项目对SOC的需求主要体现在安全管理方面，同时还要顾及与现有网管系统和工单系统的接口进行对接。

东软NetEye SOC解决方案的优势：

1、丰富的政府行业经验

东软NetEye SOC产品先后成功应用于国家信息中心核心政务外网、财政部、环保部、工信部、文化部、中科院、北京政务信息监控中心、青岛国税等关键政府行业用户中，是目前国内较为先进、成功案例较多、部署规模较大的综合监控运维管理平台。

2、产品具有多维的视角展示与操作

以往的安全运维管理平台只提供一种视角，即面向技术的视角，较为单一。安全状况多采用数字、文字、图表等方式进行描述，表达晦涩、美观度较差、不支撑宏观决策分析。东软NetEye SOC平台提供了管理、技术、业务、运维四个展示与操作视角，以更为生动、美观、简洁明了的方式展现安全状况。

东软NetEye SOC系统试图以一种全新的视角来诠释监控数据分析结果的展示。我们创新采用了以天气预报中的晴雨表的方式形象化比拟被监控对象的安全状况，分别用晴天、多云、阴天、小雨、和大雨五种天气预报来比喻从很低到很高的五个不同等级的安全状况。在原有技术支撑的基础上，用晴雨表这种人性化形态来看待安全，使SOC系统的宏观展示效果更为美观和直观。

技术视角面向安全运维人员，提供事件分析等详细的数据和资产录入的细节，便于运维人员进行全面的系统运维。

业务视角面向运维人员，采用业务建模和业务视图展示每个业务系统的IT支撑资源，并对IT支撑资源的PKI指标进行实时监控，使其可以整体关注每个业务系统的运行情况。一旦业务系统异常，可以快速定位到具体的IT支撑资源。

3、智能引擎进行海量数据的收集和分析

东软NetEye SOC系统的数据采集引擎支持分布式部署，从而实现海量数据的收集与分析。系统通过在分布式部署的数据采集引擎和中心服务器上配置的收集、分析策略实现对海量异构数据进行过滤、归并、分析和处理，大量过滤重复、无效数据。目前，在较大的项目实施中，东软NetEye SOC每天收集的原始日志最高可达到几十亿条，通过不断积累完善的归并、分析策略，平台每日上报的有效报警数据通过关联后却可以控制在有效阅读的范围之内，便于管理员把握住运维重点。当需要进行深入数据分析时，可随时将保存在数据采集引擎上的原始日志上调到中心，内置11000条事件规则以备关联分析使用。对第三方产品的支持面已经非常广，包括安全设备、网络设备、操作系统、中间件、数据库、机房环动等的产品和系统的类型已经达到130余种。

4、先进的业务应用监控

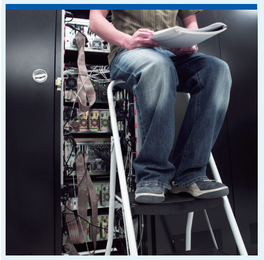
业务应用建模以应用系统为核心，在全面管理每个应用系统的IT资源的基础上，能够从网络和应用两个维度建立应用系统视图模型。用户可根据应用系统视图模型直观形象的了解支撑应用系统运行的IT资源组成情况。

应用视图管理是在应用视图模型基础上构建应用系统的资源实例和指标之间的逻辑拓扑关联关系，用户可随时调整资源实例和指标，但不损坏原有视图模型。用户可根据应用视图直观形象的了解应用系统的运行情况，能够快速定位应用系统的性能运行瓶颈及故障所在。应用视图能够展现应用系统各组成部分的运行状态、KPI指标以及业务应用告警等信息，从而展示应用系统的运行状态信息。

应用视图中实时刷新业务应用和业务节点相关的资源实例的健康状态，以不同颜色显示不同的健康状态，应用系统及其资源实例一旦出现异常告警事件，用户可直接从视图中查看告警事件信息、配置信息和运行状态。

UTM：一片仍需坚守的阵地

◎《电脑商情报》 苏畅



统一威胁管理UTM（Unified Threat Management）作为纵横在安全硬件设备市场十年之久的产品，凭借其融合的产品特性和可靠的硬件平台，早已圈定了其在安全市场中固有的领地。如今，在下一代防火墙热闹上市的时间里，UTM却成为了箭靶和亟待颠覆的目标，升级、更迭的口号不绝于耳，部分UTM主流厂商也调转枪头走向另一市场。但当呼喊声淹没在市场中后我们发现，UTM依然在保持增长势头不变，这仍是一片需要坚守的阵地。

UTM与NGFW之争

随着网络中的应用越来越复杂，安全问题以出人意料的速度增长，并且在攻击方式、攻击目标上亦呈多样化发展趋势。如何使复杂变成简单，成为网络管理人员的一个困惑。UTM就是在这种背景下应运而生的，它的定义是将多种安全能力（尤其是传统上讲的防火墙能力、防病毒能力、攻击保护能力）融合在一个产品之中，实现防御一体化，这样就为简化安全解决方案、规避设备兼容性问题、简化安全管理提供了先决条件。因此，全面的立体防御是UTM存在的理由，更是UTM发展的方向。

当为了应对当前与未来新一代的网络安全威胁而对传统防火墙进行的一次改头换面的下一代防火墙NGFW出现之后，对UTM的攻击似乎从未停止，大有把UTM当成箭靶和亟待颠覆的目标的势头，而对UTM升级、更迭的口号不绝于耳。当部分主流厂商陆续推出下一代防火墙产品的同时，UTM在市场舆论中似乎走入了困境。

被NGFW诟病的UTM的不足之处无非是众人认为UTM是将防火墙、IPS、AV进行简单的功能堆砌，功能全部开放时的效率非常低下。仔细来看，NGFW主要功能是" 防火墙+IPS+应用控制 ",其特性是在性能上大幅度提升，所有新推NGFW的厂商，其比拼都体现在防火墙的速度上。但现在的UTM,其功能不仅包括NGFW的功能，还包括反病毒、反垃圾邮件、内容过滤、防数据泄露等多个功能，并且，经过几年时间的发展，UTM性能已经大大提升和完善。

从技术本质上来说，NGFW和UTM都是采用同样的技术手段，许多厂商的核心都是采用通用CPU架构，其中又分别包括X86和MIPS架构，某些采用了NP（网络处理器）对网络层应用进行加速。虽然厂商实现的技术手段略有差异，但总体差别不大。

坚守之后带来的稳速增长

发展至今UTM硬件架构经历了ASIC、FPGA、NP、多NP、X86+ASIC/NP混合、多核等多种架构。在硬件处理性能大幅提高的同时，软件平台和安全引擎上也得到各大厂商的重视，如：研发安全设备专用的OS,重新设计的统一安全引擎或统一模式匹配引擎、多通道并行匹配引擎等，使UTM全部功能开启后仍然可用，并保持性能稳定。通过软硬件开发的努力，UTM性能瓶颈获得突破。

根据IDC最新的报告显示，与2011年同期相比，全球安全设备市场营收同比增长了5.7%，在2012年已超过200亿美元;同时，安全设备的出货量增长了1%，达到了499022台。同比2011年第二季度，2012年第二季度的全球安全设备营收增长6.6%，设备出货量增长5.8%。以功能计，统一威胁管理(UTM)是年同比增长最高的领域，其增长率为24.3%，其营收占总体安全收入的33.3%。

如今提供综合安全网关产品的厂商今天已经分化成两大阵营，一种是始终坚持自主研发综合安全网关全部功能的厂商，一种是部分或全部从第三方OEM的厂商。后者由于产品性能较低已经很难在高速互联网发达的今天满足大流量处理要求，前者则依托全自主研发的统一软件架构实现性能卓越和功能灵活多变，并逐渐在市场竞争中拉开了与后者的距离。在UTM技术的推动下，用户对综合安全网关产品的需求也在不断进化，用户越来越希望使用的设备不再只是集成大量功能模块，策略规则复杂，产生一大堆告警和日志的防护设备，而是希望能对整个互联网数据流体系结构提供全方位控制及预测，并且控制结果可随时呈现的设备。

2010年统一威胁管理(UTM)市场9.72亿美元，在2011年已经突破12亿美元大关，在2012年这个数字在14亿美元左右。这在很大程度上是源于注重预算的客户、产品添加到UTM设备以及该设备对网络整合和合规的总体支持。

国产UTM的崛起

近期，东软NetEye万兆集成安全网关NISG（IPv6版）获得国家信息安全测评信息技术产品安全测评EAL3级证书，同时成功入选国家发改委下一代互联网信息安全专项UTM类产品测试名单。

东软NISG系列是基于东软十多年的安全网关研发经验，久经市场考验的UTM类产品。该系列产品具备了丰富的安全网关功能，包括防火墙、VPN功能、防病毒功能、防垃圾邮件功能、URL过滤功能、IPS功能等。同时，具备强大的虚拟安全网关功能。一台物理设备可以模拟出最大255台虚拟逻辑设备。各个虚拟设备之间互不影响，可以单独使用防火墙功能等所有独立功能项目。其次，东软NISG支持对数百种常用和流行的应用的识别，包括即时通讯工具、Web应用、P2P下载工具、网络电视、流媒体、网络游戏、炒股软件、远程登录攻击、加密代理软件、邮件客户端等各种网络流行的应用进行细粒度的识别进而实现相应的控制。

全球IDS/IPS市场快速增长，2017年市场或超160亿美元

◎《通信世界》 黄海峰

当前入侵检测/防御硬件产品需求旺盛，但随着客户面临的威胁越来越复杂，产品也开始呈现多样化。

根据MarketsandMarkets的最新市场调查，全球入侵检测和预防系统(IDS/IPS)硬件市场到2017年将达到166.3亿美元，并在2012年至2017年间达到7%的年复合增长率。对于IDS/IPS产品市场国内发展，一位安全厂商人士介绍，相比同期数据，2012年国内市场规模稳定提高，但扩展速度在放缓，主要生产厂商基本可获得每年1~2亿元人民币左右的合同额。

IDS/IPS作为企业网络防火墙后的第二道防护措施，通过对网络状况的实时监听，从而能够与对于内部攻击、误操作、外部攻击等进行防护，从而大大提高网络的安全性。

国内市场增速或将放缓

根据MarketsandMarkets调查，美国市场在IDS/IPS市场中一路领先，紧随其后的是亚太地区和欧洲，其余市场中最大的则数中东和非洲市场。

根据技术的不同，IDS/IPS可细分为入侵者警报、边界安全及门禁等市场。每一个技术领域又根据其类型、应用和地域进一步进行划分。

随着客户面临的威胁越来越复杂，对入侵检测和预防的需求也开始呈现多样化。中东和非洲突然爆发的内乱促使政府和企业重新审视其安防措施。在亚太地区，停滞的建设项目纷纷复苏，基础建设方兴未艾，这些都为IDS/IPS解决方案提供商带来了新的商机。

专业的入侵检测/防御硬件产品需求旺盛，如据咨询机构IDC数据显示，中国入侵防御硬件市场2012年上半年同比增长15.9%，市场规模达到3880万美元。

多家国内外企业组成竞争激烈的国内市场格局。近两年，多家该细分市场领先企业推出更高性能和更多功能的IPS/IDS新产品。

“2012年IDS/IPS产品市场增速放缓。”东软网络安全资深产品经理姚伟栋认为虽然市场将快速增加，但是相比以前增速放缓。主要的影响因素：产品单价在下降，而且幅度较大；产品边界越来越模糊，各种新奇技术概念正在进入用户视野，这在一定程度上分流了固有市场份额，IDS/IPS在掠夺传统安全网关类产品市场空间的同时，也在承受着来自应用型安全网关的蚕食；IDS/IPS自身热度在降低、技术形态日渐成熟。

客户需求呈现多样化趋势

着眼未来，IDS/IPS也一定会像其他信息产品一样不可避免的去进化、去演变，性能上会越来越高，所承担的防护职责也会越来越多，尤其是针对应用层行为合规性的检测深度也会越来越强、而控制机制则会变得更加具有弹性和智能化。

“任何人在舍运面前都没有豁免权，IDS/IPS同样如此。”对于未来IDS/IPS何种产品将成主流的问题，姚伟栋表示，未来不会是某类产品消失、另一类产品取而代之，而是相互融合，即便不再有IDS/IPS这个名称，但一定会有其他的I x S继承其衣钵，而IDS/IPS的技术精髓将会在信息安全体系中持续发挥着作用。

在移动互联网和云计算大发展情况下，入侵检测/防御硬件下一步发展方向是什么？姚伟栋介绍，对于移动互联网业务，IDS/IPS必须更加精细化，更新升级也在同步加速，应做到每种主流移动应用推出之后3个月内即可提供相应的功能模块。

云计算的应用则要求IDS/IPS能够真正的部署到云内部的合理节点上，这就要求IDS/IPS能够识别、理解云的构造并对其数据流进行解读控制，这势必将引入新的规程协议，这要求包括IDS/IPS在内的所有周边配置机制伴随着“云”共同成长，毕竟目前众说纷“云”，而且变幻莫测、不可捉摸，即使是当事者也难以预测到底哪块“云”能下雨。

三问安全厂商

——对话东软网络安全营销中心资深产品经理 姚伟栋

《通信世界》：从产品角度看，传统入侵检测/防御硬件产品存在哪些挑战？新的产品需求呈现哪些特点？

姚伟栋：传统IDS/IPS产品主要侧重于攻击行为的检测，而目前市场则要求提供更多的针对应用层尤其是其特有业务的行为检测，这是IDS/IPS所面临的主要挑战。

这些新需求呈现出的特点主要是每个行业、每个客户都要求一定程度的可定制性，每个大型行业都有自己独有的应用业务，即便是同样运行在HTTP上的不同应用，也要求更加针对性的检测控制能力，原先IDS/IPS所提供的针对HTTP@TCP@IP的检测原理已基本失效，进而需要提供的是SpecialAPP@HTTP@TCP@IP的检测控制模块，这就是新需求的特点。

《通信世界》：2013年，入侵检测/防御硬件产品和市场机遇无限。贵公司认为安全企业应该如何做规划？

姚伟栋：2013年，我们将在IDS/IPS方面主要进行两部分的规划。

其一，有效的将物理上的单板进行高耦合度的集群，无论是在GUI界面上还是在后台CLI界面上都应该向管理员呈现出统一的管理接口，每块单板应像是普通外设板卡一样，而不应该具备独立的操作系统地位；

其二，我们将持续加大在应用协议方面的扩容，一方面要依靠东软NetEye安全实验室的技术积累不断推出新的应用防护模块，另一方面更要完善用户自定义应用防护相关功能。

《通信世界》：通信行业客户对该产品需求有哪些特点？

姚伟栋：如同其他特大型行业客户一样，通信行业每个需求都有可能影响IDS/IPS技术形态的演变节奏。移动通信的各种应用业务，如彩信、WLAN、短信、IM都开始逐步考虑IDS/IPS对之提供针对性的检测控制模块。