中国上网行为管理蓝皮书

深信服科技

目录

观点

2009，中国上网行为管理市场经历了高速发展的一年。据 IDC 调查显示，受到金融危机影响，一些主流厂商甚至在某些季度出现了负增长，而上网行为管理领域中，仅“web 过滤和信息安全产品”这一细分领域未来五年的预期复合增长率高达 36.0%，成为所有安全硬件市场中增长最快市场的之一。

尽管国家相关部门尚未对“上网行为管理”这一概念做出明确定义和评判标准，但并未影响市场对上网行为管理类产品的强烈需求。经过近五年来市场与客户的层层选择，一些优秀的上网行管理厂商逐渐崭露头角，成为市场领导者，他们所采用的技术、所定义的产品功能已经成为业内共识的风向标。

关于本蓝皮书

本书宗旨

深信服科技作为前沿网络领域的领导厂商，于 2005 年推出中国第一台专业的上网行为管理网关，并定义了上网行为管理产品的核心功能。多年来，深信服致力于帮助用户的业务向互联网转型，提升带宽价值，并根据用户的业务需求不断改进和完善产品。

本书中，深信服科技深入研究了一百个具有代表意义的网络样本，分析其网络应用现状和网络所处环境，以图表形式展示调查结果并加以解读。在此基础上，深信服结合多年的产品研发经验，阐述专业上网行为管理产品应为客户提供怎样的应用价值，以及需具备的基础功能与高级功能，期冀与读者共同探寻上网行为管理领域的未来技术趋势和产品走向。

附录中，深信服提供了部分典型客户的案例详解、企业网网络管理指导书、产品选购指导等，旨在为客户提供网络安全管理办法与参考建议，帮助客户制定适合组织文化与网络现状的 IT 管理制度，并采用相关技术手段保障制度的有效实施。

相关数据来源机构介绍

CNNIC：中国互联网络信息中心（China Internet Network Information Center，CNNIC），负责管理维护中国互联网地址系统，权威发布中国互联网统计信息，代表中国参与国际互联网社群。

IDC：国际数据公司（International Data Corporation），全球著名的信息技术、电信行业和消费科技市场咨询、顾问和活动服务专业提供商。

厂商背景

深信服科技有限公司是中国规模最大、创新能力最强的前沿网络产品供应商，致力于通过创新、高品质的产品及卓越的服务，帮助用户的业务向互联网转型。

作为一家专注于广域网市场的厂商，深信服提供了贯穿用户广域网建设生命周期的前沿产品及解决方案，包括上网行为管理、IPSec VPN、SSL VPN、广域网加速、应用交付、流量控制、上网优化等，并被公认为多个领域的技术及市场领导者。

截止 2010 年 5 月，已有超过 16,000 家用户成为深信服的合作伙伴，包括通用电气、壳牌石油、丰田汽车、中国移动等世界知名企业，以及中国人民银行、国资委、国土资源部、外交部等重要政府机构。

据 IDC《中国 IT 安全硬件市场分析与预测》（2009 年下半年）调查报告显示，深信服上网行为管理网关以 33.8%的市场占有率，排名“安全内容管理硬件”市场第一。

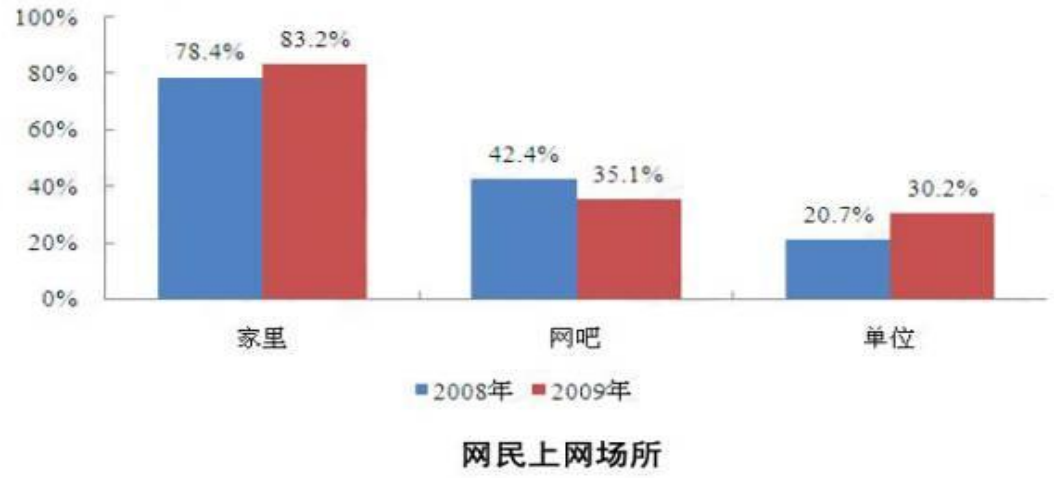
目前，深信服公司总人数 900 余人，国内直属分支机构 34 个，并在香港、新加坡、阿联酋、泰国、印度、英国等国家和地区设有海外直属办事机构。

一、上网行为管理综述

环境与趋势

据 CNNIC《第 25 次中国互联网络发展状况统计报告》（报告时间：2010 年 1 月）显示：

- 截至 2009 年 12 月 30 日，中国网民规模达到 3.84 亿人，网络普及率达 28.9%；
- 网民在单位上网的比例明显提升，30.2%的网民在单位上网，2009 年在单位上网的网民数量增加量超 5000 万，互联网作为生活工具和工作工具的价值进一步提升；



网民上网场所

图片来源：CNNIC《第 25 次中国互联网络发展状况统计报告》，第 29 页

- 随着便携式电脑以 42.4%的增长率远超台式机，网络随处接入的趋势日益明显；
- 网民每周上网时长人均增加 2.1 小时，达到 18.7 小时；

2003-2009 年中国网页规模变化

图片来源：CNNIC《第 25 次中国互联网络发展状况统计报告》，第 23 页

➢ 2009 年网络应用使用率排名前三为网络音乐（83.5%），网络新闻（80.1%），搜索引擎（73.3%）；

➢ 2009 年商务交易类应用的用户规模增长最快，平均年增幅 68%，其中，网上支付用户年增幅 80.9%，在所有应用中排名第一，其次是旅游预订（77.9%）、网络炒股（67.0%）、网上银行（62.3%）、网络购物（45.9%），中国互联网影响显现从娱乐化向消费商务型转型的趋势。

表 11 各类网络应用使用状况及用户增长

类型	应用	2008 年使用率	2009 年使用率	用户增长率	使用率排名	增长率排名
网络娱乐	网络音乐	83.7%	83.5%	28.8%	1	11
信息获取	网络新闻	78.5%	80.1%	31.5%	2	9
信息获取	搜索引擎	68.0%	73.3%	38.6%	3	7
交流沟通	即时通信	75.3%	70.9%	21.6%	4	13
网络娱乐	网络游戏	62.8%	68.9%	41.5%	5	6
网络娱乐	网络视频	67.7%	62.6%	19.0%	6	14
交流沟通	博客应用	54.3%	57.7%	36.7%	7	8
交流沟通	电子邮件	56.8%	56.8%	29.0%	8	10
交流沟通	社交网站	--	45.8%	--	9	--
网络娱乐	网络文学	--	42.3%	--	10	--
交流沟通	论坛/BBS	30.7%	30.5%	28.6%	11	12
商务交易	网络购物	24.8%	28.1%	45.9%	12	5
商务交易	网上银行	19.3%	24.5%	62.3%	13	4
商务交易	网上支付	17.6%	24.5%	80.9%	14	1
商务交易	网络炒股	11.4%	14.8%	67.0%	15	3
商务交易	旅行预订	5.6%	7.9%	77.9%	16	2

图片来源：CNNIC《第 25 次中国互联网络发展状况统计报告》，第 32 页

综合 CNNIC 报告与对样本用户的研究，我们注意到如下几个趋势：

➢ 企业网上网条件有较大提升，在单位上网的网民数量大幅增加，网民将个人网络行为带入工作场所，人际关系在网络上的延伸让网络表现出社会性，并对互联网的依赖性进一步加深；

➢ 互联网应用日益丰富，并呈现从娱乐化向消费商务化转型的趋势，互联网改变生活，改变消费模式；

➢ 企业网用户对网络的要求从最基本的连通性、安全性，到追求最优的网络利用率，到利用网络开展业务，向网络要效益——在互联网影响下，产业正在向互联网转型，因此，互联网双向访问稳定与安全的重要性日益凸显；

➢ 一方面，信息量急速膨胀，信息传播途径多样化、传播速度呈几何级数增长；另一方面信息质量良莠不齐、鱼龙混杂，信息的筛选与过滤目前缺乏统一评判标准；

- 互联网安全管理的趋势：今日互联网的威胁主要集中于内容威胁方面，诸如窃取用户资料，盗取账号密码，攻击其他计算机以获取经济利益的行为。传统专注于网络层 TCP/IP3 层、4 层的管理防范手段已无法有效应对，网络安全管理的重点已然转移到以应用内容为主的 7 层防护上；
- 国家关于互联网管理的法律、法规、公约，行业主管部门关于行业网络监管的管理指导、管控规范等陆续出台，国家对互联网管理力度逐步增大。

综上，企业网用户面对互联网带来的种种机遇和挑战，产生了对网络应用效率、网络管理质量、信息安全防护、满足法规政策多方面需求，加速了上网行为管理产品市场的发展。

产品定义

从产品形态看，上网行为管理产品可分为软件、硬件两大类，由于硬件产品具有易部署、易维护、稳定性高、更安全等特点，已成为市场主流。在硬件网络产品中，存在 X86、ASIC、NP 三种架构，由于上网行为管理产品涉及大量应用层、内容级的复杂逻辑运算与处理，所以 X86 架构独具的开发灵活性、复杂运算适应性使得 X86 架构成为上网行为管理的首选，加上英特尔不断发布集成度更高、性能更强劲的处理器，俨然使得 X86 架构成为上网行为管理硬件产品的不二之选。

上网行为管理硬件网关，根据适用规模不同，又可分为企业级产品和电信级产品。部分中小厂商由于实力有限，其目标客户集中于中小企业，型号覆盖面较窄，产品性能及功能完善程度不足；部分领导厂商产品覆盖面较广，不仅有适用中小网络规模组织的小型产品，更有适应运营商级别网络规模的高端产品。

带有初级上网行为管理功能的硬件网关出现在 2004 年前后，早期产品多以 UTM（统一威胁管理网关）、多功能防火墙、多功能网关等名称出现。随着客户需求的不断明晰和厂商的技术积累，上网行为管理这一细分市场逐渐独立、形成并发展起来。区别于传统的基础网络产品（防火墙、路由、交换产品等），上网行为管理产品作用于应用层，基于对应用协议/内容的识别进行管控，因此识别能力是评价上网行为管理产品优劣的重要指标。

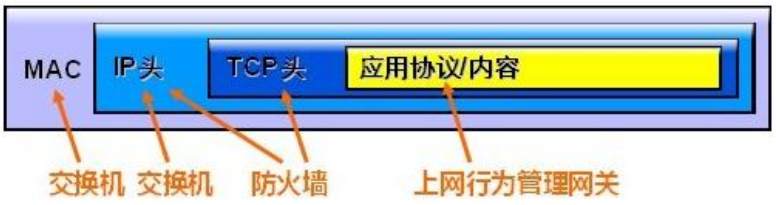


图 1 上网行为管理产品识别层次

经过多年市场筛选，上网行为管理产品明确了身份认证、应用权限控制、流量管理、内容过滤、应用行为记录、数据分析、安全防护等基础功能，帮助客户实现内网统一身份认证，管控组织网络应用，提高员工工作效率，实现与职权匹配的访问权限分配，优化带宽管理，提升网访问质量，保护组织信息安全，

防范业务风险，规避违规行为带来的法律与舆论风险，提高内网安全级别等目的。

近年来，随着客户的高级需求、特别是高端客户需求的不断涌现，推动高级上网行为管理产品开始融合终端安全检测、局域网准入控制、内网访问流量控制等功能。

图 2 主流上网行为管理产品功能一览

二、企业网网络管理现状

All On Internet

对企业网用户而言，“广域网”概念涵盖两方面：内部的专网与外部的互联网。随着各运营商竞争加剧，专网带宽越来越大，价格越来越便宜，但专网形态的变化并未改变其原有的作用。但变化中的外部互联网，却对企业网用户的业务造成着广泛而深远的影响。

未来十年将是“All On Internet”的十年：即语音、视频、数据、应用等应用都会基于互联网，广电网、电信网、互联网三网合一就是这一趋势的最大明证。这个趋势将使得未来客户的所有应用都将迁移到互联网上，而基于互联网的应用会更趋向 Web 化。

正如前面所述，互联网改变生活、互联网改变产业——企业网用户在面临互联网环境变化带来的机遇和挑战的同时，对网络的要求从基本的连通性、安全性，到追求最优的网络利用率，直至到向网络要效益——我们清楚地看到，在互联网影响下，企业网用户的业务正在向互联网转型，这种趋势使得互联网质量保证和安全保证愈加重要。

网络管理现状分析

然而，企业网用户能否驾驭、并用好互联网？对互联网风险的防御力如何？提高网络质量和安全级别应该从哪些方面着手？

2008 年 6 月 28 日，财政部、证监会、审计署、银监会、保监会联合发布有“中国版萨班斯法案”之称的《企业内部控制基本规范》，目的在于加强和规范企业内部控制，提高企业经营管理水平和风险防范能力，促进企业可持续发展。2009 年 7 月 1 日，该《规范》率先在境外上市的企业中生效施行，到 2010 年 1 月 1 日境内上市企业亦开始施行并遵从该《规范》。

然而，据德勤在 2008 年和 2009 年连续两年对国内上市公司的内部控制实施状况跟踪调查发现，有 56%的公司没有建立或现有内部控制机制尚不完善，72%的公司认为自身没有持续监控内部控制的有效机制，与 2007 年相比，企业内容在持续监控方面没有得到显著改善。

上述数据说明，仅仅依靠制度无法达到预期效果，需要采用技术手段加以保障。《企业内部控制基本规范》虽然目前只对上市公司提出明确要求，但是，它从“内部环境、风险评估、控制措施、信息与沟通、监督检查”五方面提出的指导意见，对所有组织的管理均存在重大的指导意义。

据此，2009 年 1 月，我们调查了北京、上海、广州、深圳、杭州、南京等地的数百家网络规模在 500~12000 人之间，带宽从 100M 到 1G 的组织的网络管理状况，涵盖政府、教育科研、金融、运营商、能源、医疗、大中型企业等行业，从中抽取了 100 份有效调查结果，其中仅有 26 家单位部署了上网行为管理硬件产品。2010 年 1 月，我们对这些组织进行了回访，其中已有 78 家单位部署上网行为管理硬件产品。

我们将在下文整理对比、并以图表展现以上变化，同时分析解读深层原因。

组织 IT 制度

一个单位的组织文化、组织架构、业务组成、管理风格、所处行业背景、已有网络环境、IT 投资规划等，影响着单位的 IT 管理制度和主管单位对其的信息安全等级要求、信息安全保密要求，影响管控的严格程度。

我们着重探究与管理直接相关的 IT 制度的制定和执行情况。数据显示，被调研的 100 家组织的 IT 制度的制定和执行情况在一年中有明显改善：上网行为管理产品的实施促进了 IT 制度成型，管理制度的完善程度达到 68%，相比 2009 年的 48%有较大提升。

我们将现行 IT 制度的执行情况分为三个等级：“良好”为用户了解并自觉遵守相关规定，制度执行无障碍，所采用的技术足以支撑现行制度；“一般”为用户了解并接受相关规定，执行遭遇阻力较小，所采用的技术与现行制度稍有偏差；“较差”为用户不了解或了解但不接受、不遵循相关规定，执行阻力大，未明确配套技术保障。2010 年有 66%的 IT 管理员认为组织的现行 IT 制度执行效果“良好”，这一满意度大大高于 2009 年的 27%。

解读：*“三分制度、七分管理”，缺乏技术手段支撑的管理制度就像一道没有装锁的门，只能依赖人工值守或被管理者的自觉遵守。越来越多的 IT 管理员意识到，必须选择适合组织 IT 环境的技术手段，才不会让管理制度流于形式，规范网络管理对于减少 IT 管理员的无谓工作量，优化网络环境，提升内网安全有重要意义。*

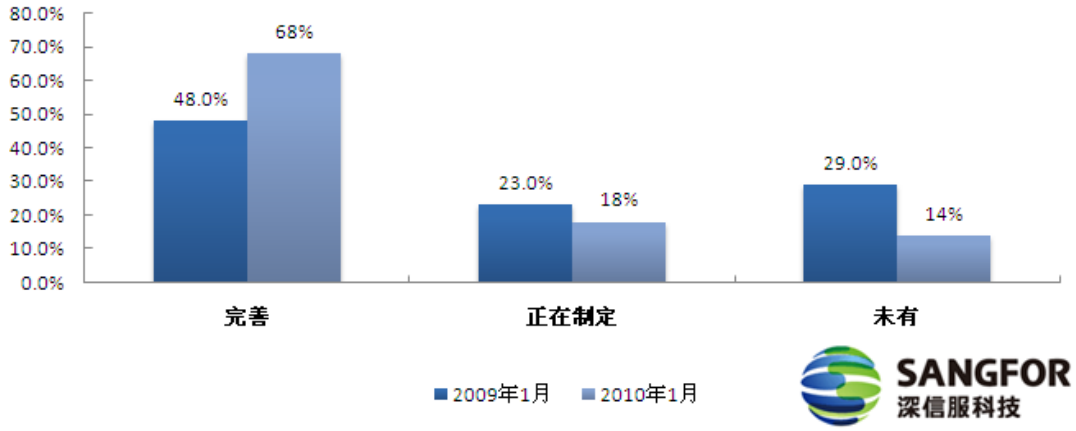


图 3 ：2009-2010 IT 制度制定情况对比

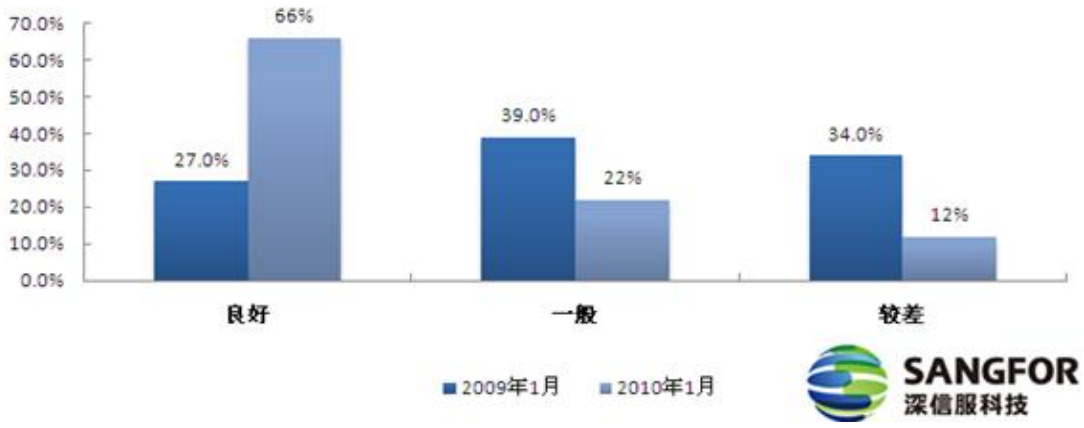


图 4 ：2009-2010 IT 制度执行情况对比

风险评估

缺乏管理的网络会让组织面临管理困难和业务风险，管理漏洞主要集中在如下几个方面：

- 来自组织内部的风险

✓ 对接入用户的身份认定

尽管大多数组织对于接入内网的用户都有相关的管理规定，然而，我们在 2009 年的调查中发现，许多组织并未强制执行。“强制认证”包括终端 IP/MAC 绑定、到认证服务器认证（包括且不限于到管理网关认证，使用 AD 域、LDAP、Radius、邮件服务器、Proxy、802.1x 等认证）、终端硬件资产认证等等。在 2009 年的调查中，仅有 11%的组织严格要求，“要求但不强制认证”即管理制度中有相关规定，但实际操作中未采用任何措施，“无需认证”即没有要求认证，无需输入用户名密码、使用透明代理、直接通过路由器等方式自由上网。

2010 年的调查数据呈现较大改观，有 45%的组织加大对接入用户的身份管控，新增数据大部分来自“要求但不强制认证”的组织。

解读：*没有严格的认证体系就无法有效区分用户，差异化管理亦无从谈起，更无法有效防范诸如身份冒充、权限扩散与滥用等风险。在 2009 年，众多 IT 管理员未采取必要的技术手段以保证管理的基础：用户识别，为了方便，有的组织甚至未采用任何认证手段；随着越来越多的管理者在网络管理、安全防范等方面意识的增强，用户身份认定成为首要解决的问题。这一变化使得强制执行身份认证机制在 2010 年成为中高端用户的主流选择。*

在身份认证中，用户使用容易被破解的密码，或长期使用相同的密码，导致认证机制形同虚设的情况屡见不鲜。为此，IT 管理员也在积极寻找解决之道。

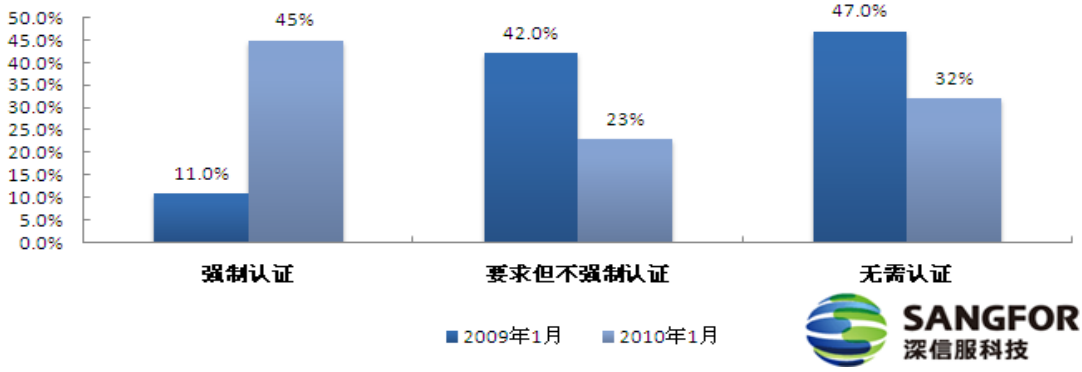


图 5：2009-2010 接入用户身份认证情况对比

✓ 鉴定接入终端安全级别

2009 年的调查数据显示，即使未采用强制认证手段，但仍然有过半数组织的管理者意识到其必要性。但对于接入内网终端产品的安全状况进行“评估”与“管理”的意识却相对薄弱，采用网络准入方案的组织更是少之又少，仅有 6%。尽管在 2010 年的回访调研中这一数据上升到 21%，但在整个样本中仍属少数，值得关注的是，许多组织注意到这一亟需加强的方面，有 46%的组织计划在这方面做出改善。

解读：*已感染的终端在内网肆虐并不断寻找下一个受害者，由此造成的系统中断、数据泄密、收入损失、数据损坏，给组织业务带来巨大影响。*

终端安全级别鉴定与网络准入控制方案之所以未得到广泛应用，一方面因为某些组织的高层管理者尚未意识到终端安全在安全体系建设中的重要性；一方面由于传统网络产品厂商推出的此类方案实施周期长、对已有网络的改动较大、实施成本高，非一般组织能承受。

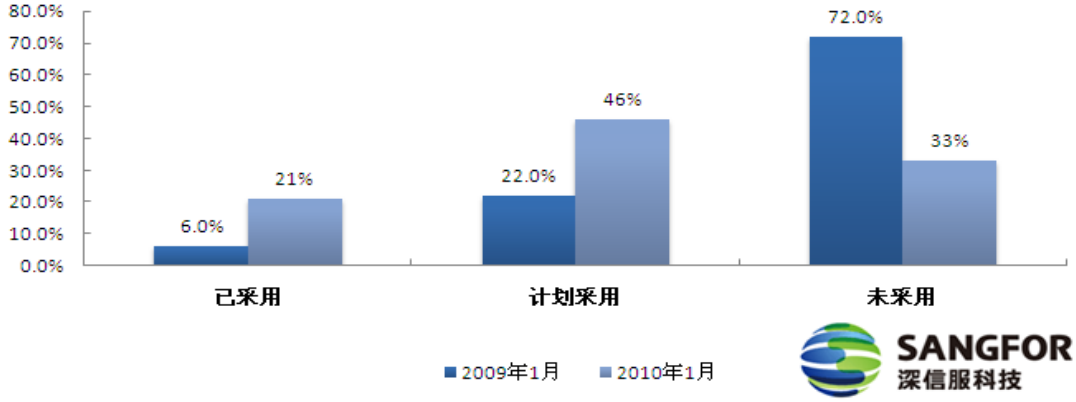


图 6 ：2009-2010 终端安全级别鉴定与准入控制情况对比

✓ 对网络应用组成的了解

2010 年，对所在组织的网络应用组成情况表示“清楚了解”的管理员比率为 71%，较 2009 年增长了 38 个百分点。从 2009 年的 82%和 2010 年的 94%，我们可以看到，绝大多数 IT 管理员都一致认同了解网络应用组成情况是十分重要的。

解读：*网络应用极其丰富，尤其随着大量社交型网络应用的出现，用户将个人网络行为带入办公场所，由此引发各种管理问题，而识别是管理的基础，对网络应用组成的了解是制定、调整管理策略的依据。*

IT 管理员对识别的重要性的认识如此一致，但是 2009 年，表示“清楚了解”的管理员只占总数的三分之一，一方面因为组织高层管理者不认为需要专业的管理产品来解决识别的问题，管理员的呼声未引起足够重视，一方面 IT 管理员在网络上可寻得一些免费管理软件，这些软件虽然能对应用流量做一些简单分析，但是存在专业度不够，识别率不高，分析层次有限，对于开启了防火墙的终端就不能分析等问题，并不能完全实现管理员希望达到的效果。

随着组织高层管理者认识到投资 IT 对组织发展的价值，逐渐支持采购专业的产品来进行管理，上网行为管理产品因其在应用识别方面的突出表现和灵活的控制手段受到 IT 管理员的青睐。

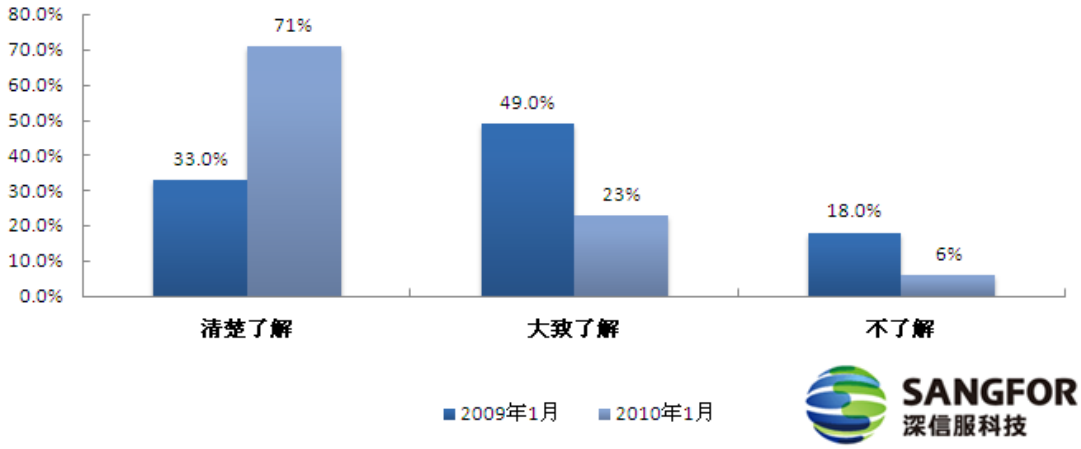


图 7：2009-2010IT 管理员对组织网络应用情况了解程度对比

2010 年 1 月，我们以网络流量的组成成分为统计对象，通过互联网上数千台深信服中高端上网行为管理产品在一月份工作时间（9:00-12:00,14:00-17:00）收集到的数据为依据，统计得出“企业网网络应用组成排名”、“企业网用户网络应用组成排名”（按大类划分），得到企业网网络应用的组成成分和带宽资源的占用率。与 CNNIC 不同，CNNIC 以网民的个人应用组成为统计对象，将网络应用分为网络娱乐、信息获取、交流沟通、商务交易四大类，结论是应用的使用率。

解读：*从统计结果，我们看到，P2P、文件下载（含迅雷下载）、P2P 流媒体等应用平均占用了 71.2%的带宽资源，网络游戏（含交友网游）、炒股等本不应该出现在办公网络的应用也出现在列表中。*

随着互联网的快速渗透，网络应用日趋丰富，网络技术特别是共享技术的发展（如迅雷推出的“协同下载”）让用户获得信息的途径和速度有了根本改变。加上各运营商之间的竞争，带宽越来越大，价格越来越便宜，几乎每个网络用户都有使用 P2P 工具获取各种影音、软件的经历。由于绝大多数组织的网络都是免费开放给员工使用的，不加控制就很容易因带宽滥用而出现各种问题。

据 CNNIC 调查，即时通讯工具使用群体主要是 30 岁以下人群，而现代组织中 30 岁以下人员同时是使用网络的主力军。即时通讯工具几乎可以说是相当一部分网民在网络上的第二身份，加上近两年兴起的社交网站、社交类游戏，将人际关系由现实向网络衍生。即便在上班时间，利用网络来实现日常交际也是许多网络用户每日的必修课，即时通讯工具的个人日均在线时长为 2.9 小时。

值得关注的是，“其他”中出现了病毒木马等异常流量，尽管所占不到 0.1%，但已足以引起我们的警惕。今日互联网的威胁主要集中在对内容的威胁上，诸如窃取用户资料，盗取账号密码，攻击其他计算机以获取经济利益的行为，用户感染各种病毒木马的概率随着各种娱乐行为的增加和安全意识不足正在逐年上升。因网络间谍入侵窃密、染毒终端异常外发数据引起的信息安全事件屡见报端。对于有保密要求的组织，尤其要注意网络异常流量的存在。

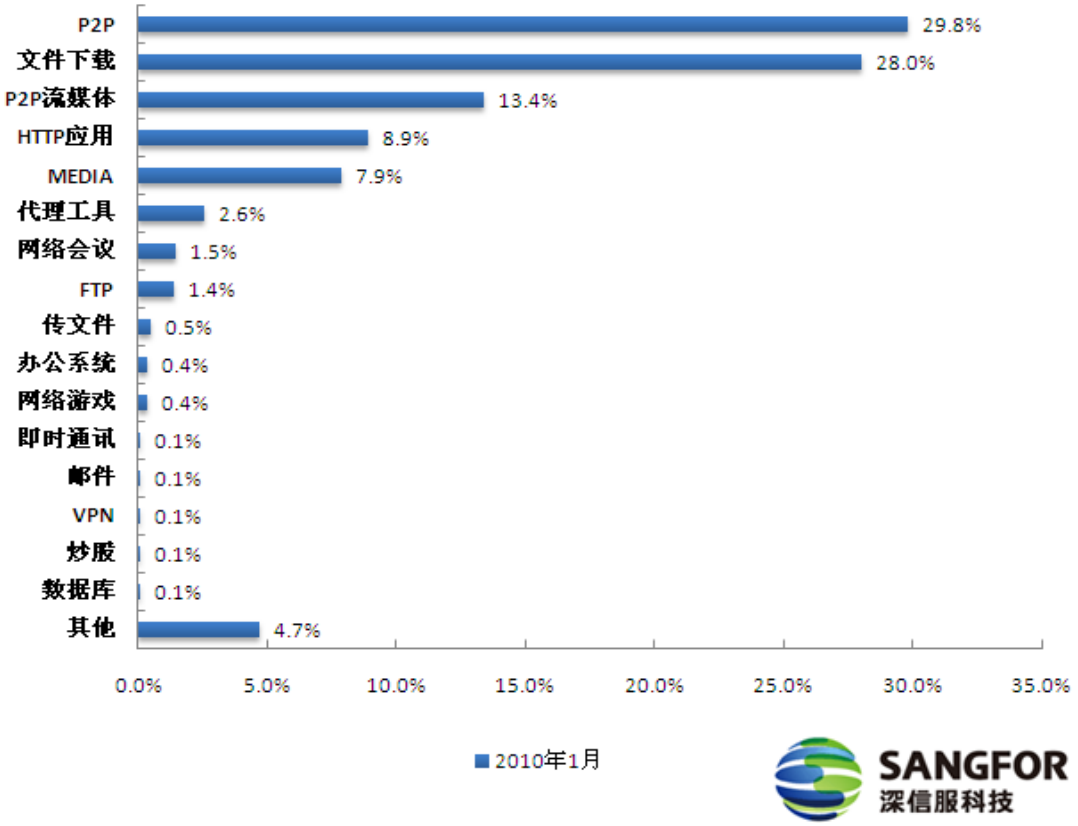


图 8：2010 企业网网络应用组成排名（按流量排名）

“文件下载”包括迅雷、多线程下载等；“传文件”包括即时通讯工具文件传输、网络硬盘等；“办公系统”包括办公 OA、ERP、CRM 等；“HTTP 应用”包括 HTTP-GET（单线程下载）、HTTP-POST、网页浏览等。“其他”中包含木马病毒流量、端口扫描、非标准端口流量、远程控制、网络共享、网上银行、其他网络协议等。不同组织对应用的管控力度存在较大差异，因此统一采用未加任何控制策略时的统计数据。

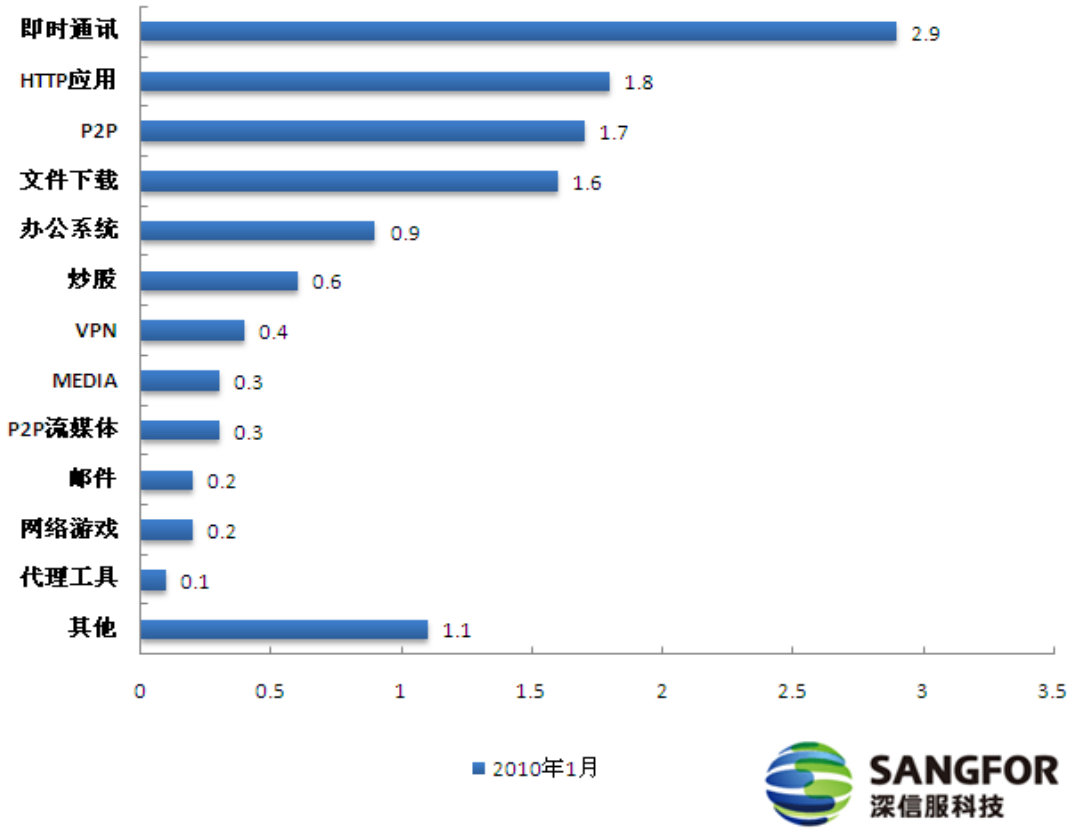


图 9：2010 企业网网络应用组成排名（单用户日均时长）

✓ 带宽资源管理方面

如图 8，我们提供了“企业网网络应用组成排名（按流量）”，其中，P2P、文件下载（含迅雷下载）、P2P 流媒体等应用平均占用了 71.2%的带宽资源。

调查发现，超过 60%的组织（将“细致控制”和“简单控制”的数据相加，2009 年为 67%，2010 年为 83%）采用了流量控制措施，证明控制以提高带宽资源应用效率是现代组织 ITIT 管理员的共识。“细致控制”指基于时间、用户组/用户、应用至少三个因素的控制；“简单控制”指基于 IP、端口的控制。

2009 年，接受调研的 100 家组织中仅有 9%使用专业的流量控制产品，其他 47%利用已有的防火墙、交换等传统产品作简单管控，44%使用了网管软件。2010 年，使用专业流控产品的组织比例上升了 52 个百分点，网管软件的使用率大幅下降。

解读：*业务不断发展，组织业务开展所需带宽与已有的带宽资源之间的矛盾越来越明显，随着业务向互联网转型，生产效率与网络利用率紧密相关，对带宽资源的管理已被许多组织列入生产资料的管理范畴。现今互联网应用的极大丰富，加上绝大多数组织的网络都是免费开放给员工使用的，几乎每个用户都有使用组织网络从互联网上获取各种影音娱乐资料、软件的经历，不加控制就很容易因滥用而出现各种问题。因此，对带宽资源的管理集中在对组织核心业务、核心人员进行带宽保障，对非业务相关应用进行限*

制两方面。

在 IT 管理员选择流控产品时，专业的流控产品逐渐取代防火墙等传统产品，一方面因为专业流控产品作用于七层，识别率与控制粒度非传统产品可以比拟，另一方面因为越来越多的 IT 管理员出于网络稳定性考虑，希望专机专用。而专业的硬件流控产品逐渐取代网管软件，因为硬件产品具有易部署、易维护、稳定性高、更安全的特点，同时软件产品本质上依然要依赖硬件（如安装在服务器或电脑上），专业的网管软件部署复杂、周期长，维护量大、成本有时比硬件还高，而免费的网管软件专业度不足，很难满足大中型网络的管理需求。

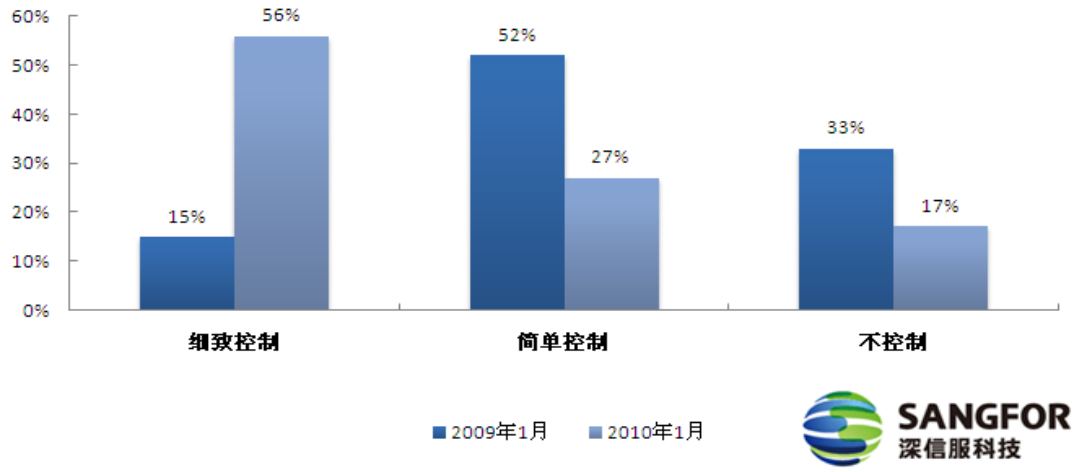


图 10：2009-2010 出口带宽流量控制情况对比

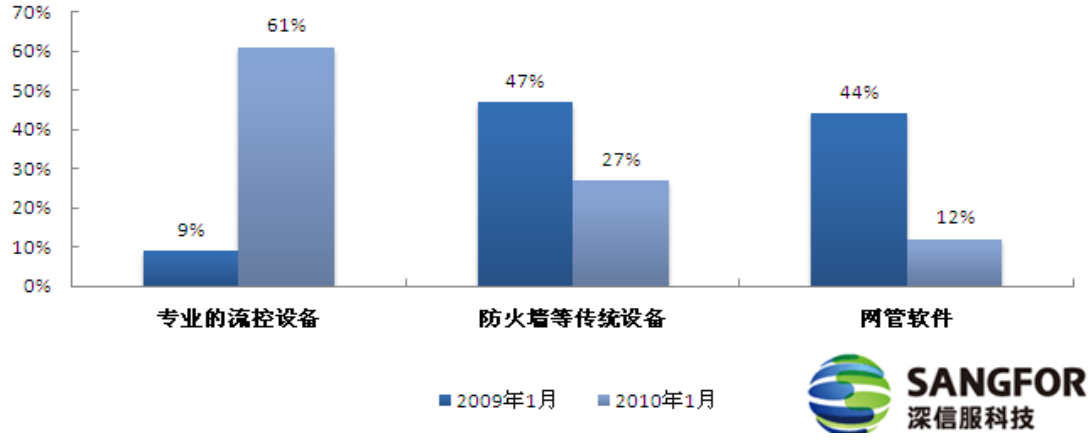


图 11：2009-2010 流量控制手段对比

✓ 网络应用权限的管理

处于不同行业的组织对网络应用权限控制的要求程度不同，图 12 的调查数据取自接受调研的组织中允

许访问互联网的网络，不一定适合所有行业，仅供参考。

2009 年，对用户网络应用权限采取“最低权限”管理的组织仅有 9%（“最低权限”即仅分配业务办公所需的权限），且这些组织是科研院所、军工单位、金融行业，尽管 2010 年这一数据有小幅上升，但仍然集中在上述几个行业。相比之下，采取“受控权限”管理的组织同比增加了 49 个百分点，增长幅度大、行业覆盖面广，此类组织在兼顾权限与职位匹配度的同时考虑了人性化的管理需求，采取弹性控制。将网络应用权限“完全开放”的组织减少了 56 个百分点，但仍然有 21%的组织使用，集中在教育行业以及二级运营商。

解读：*加强管理的组织数量大幅增加主要有两个原因：一方面许多组织管理者发现，开放网络的初衷是为了业务开展和信息互通的需要，但是缺乏对应用权限的管控导致了一系列问题：*

✧ *用户在工作时间从事与业务无关的网络活动，影响工作效率，影响他人正常办公；*

✧ *用户在浏览网页、通过网络收发文件时不慎访问挂马网站、下载带毒文件，将病毒、木马等引入内网；*

✧ *核心岗位的员工（如研发人员）、掌握组织核心机密的员工（如财务人员）权限过大，存在通过网络外发泄密信息的风险；*

✧ *用户访问了违法网站、或者浏览、转载了内容违法的网上信息导致法律问题；*

✧ *高权限用户通过代理软件等代理低权限用户上网，导致管理失效；*

✧ ……

另一方面，除了组织管理者自身管理意识提升，国家与行业管理部门的行政要求也是一个重要因素。近几年来，国家加强了对互联网的管控力度，相关的法律法规陆续出台，对拥有互联网出口的组织提出了管理等级要求。

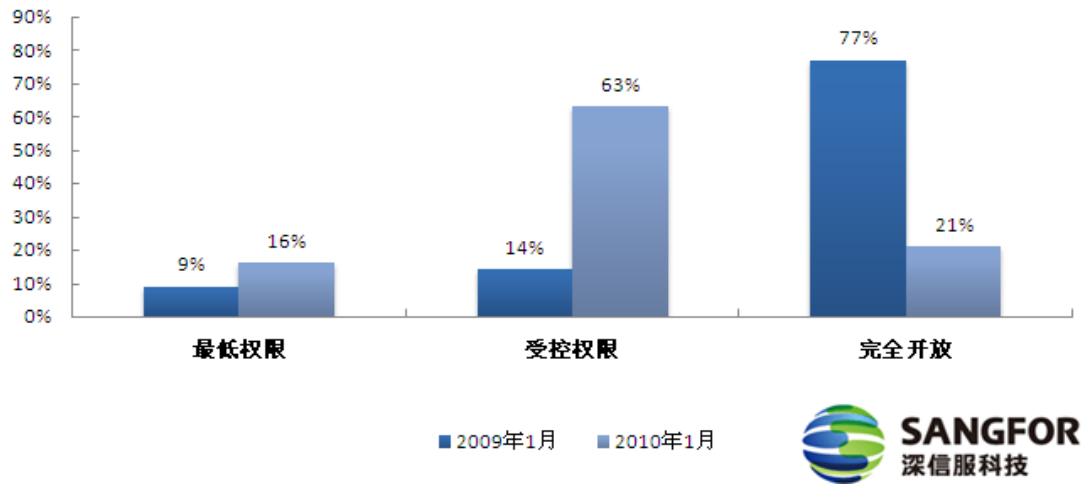


图 12：2009-2010 网络应用权限控制情况对比

“权限控制”包括但不限于：HTTP 控制（网页访问控制、发帖控制）、邮件收发权限控制（包括邮

件用户端与 webmail）、上网时间/上网流量限制、应用服务权限控制（即时通讯、P2P 应用、炒股、FTP、在线流媒体、网络游戏等）、代理工具控制、办公系统访问权限控制。

✓ 对网络行为的记录

对用户网络行为“完全记录”的组织在两次调查中均属少数，我们不做过多关注，将注意力集中在“部分记录”和“不记录”两项。“部分记录”指组织对用户网络行为有选择地进行记录，依据可以是用户所在职位要求、涉密级别要求、国家相关法规以及网络监管部门要求等。

2009 年，70%的组织没有使用网络行为记录方案，但这些组织在 2010 年大量部署相关方案，采用“部分记录”的组织从 28%增长到 72%。

解读：*对用户网络行为的记录一直是一个颇有争议的话题，采用网络行为记录方案的组织大幅增加的原因主要有两个：一方面国家为了净化互联网环境，逐步建立对互联网行业发展的市场规范，监管力度不断增强；另一方面，组织出于自身信息安全保护的需求：如防止信息资产泄密、预防舆论风险、保留安全事件的相关证据，以及管理上的要求，如考核员工的网络工作效率、分析网络应用情况、提供管理依据等，也会部署行为记录方案。*

2009 年的调查中我们发现，许多组织管理者对于部署行为记录方案可能遭遇的管理阻力和舆论阻力表示担忧，主要来自“如何避免对关键人员（如组织高层领导）的过度记录”、“如何实现对日志的保护和保密”、“如何控制对日志的访问和查看权限”三方面，并希望方案提供商能给出合理的解决方法。

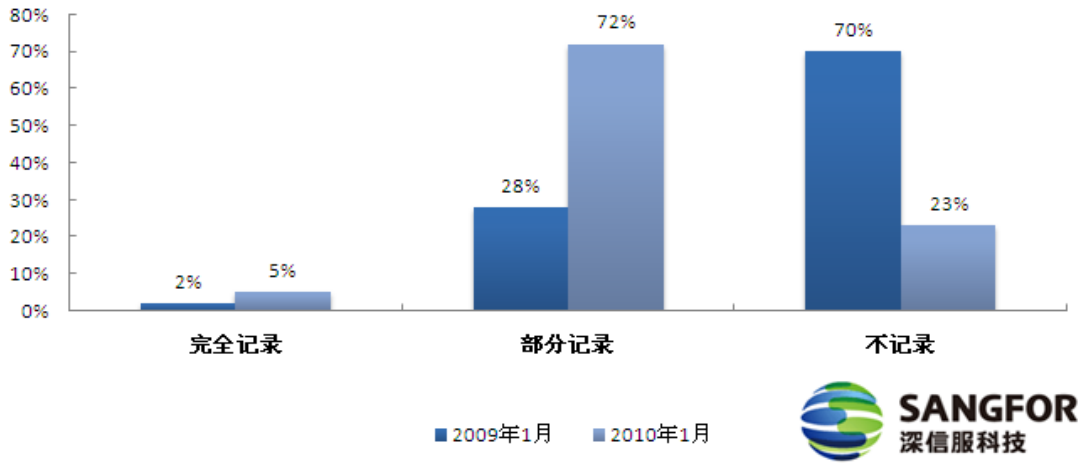


图 13：2009-2010 网络行为记录方案部署情况对比

“网络行为记录”包括：网页浏览、BBS/BLOG 发帖、邮件收发行为（包括邮件用户端与 webmail）、应用服务使用情况（P2P 应用、炒股、在线流媒体、网络游戏、其他网络协议等）、文件收发行为等。

➢ 来自外部的安全威胁

来自网络的安全威胁如：病毒传播、网页/邮件挂马、黑客入侵、垃圾广告推送、网络数据窃贼等，造成的资料泄密，系统瘫痪状况已成为各行业信息化建设中的重要问题。

2010 年的调查数据显示，66%的 IT 管理员接到因用户访问挂马、携带恶意插件、脚本的网页、邮件引起的告警，接近 50%的 IT 管理员接到用户反馈受到内网病毒木马和垃圾信息的困扰，31%的 IT 管理员曾经发现网络攻击和入侵行为，26%的组织曾经发生内部资料外泄、单位及个人信息泄露，还有 17%的组织曾经发生过服务器遭受攻击的安全事件。

解读：*据相关报告统计，每 600 个 PDF 文件中就有一个带有恶意软件、每 2000 个 JavaScript 文件中就有一个携带恶意软件。如果乘以互联网的庞大基数，得出的数字难以想象的。*

由于网络犯罪成功率高、非法获利大，对组织网络的安全威胁也是日新月异，并且更加善用伪装：利用社交网络散播，仿冒可信网站，将访问合法网站的用户“重定向”到非法网站，假冒可信软件如防病毒软件、插入非法软件，通过恶意广告、垃圾博客、恶意点对点文件传播等等。当用户发现时，用户端已经被安装恶意插件，被强迫浏览黑客指定的网站，或者被利用攻击某个站点，终端信息已被外发，损失已造成。

而传统防范措施均建立在对已知威胁的了解上，带有一定滞后性，许多威胁并不能单靠特征式、类似防病毒技术来防御，终端用户和 IT 管理员必须在自我防护方面始终保持警惕：坚持将软件更新至最新版本、部署全面的端点安全产品、保持警觉并采用高强度密码策略、采用网络准入技术鉴定并隔离不同安全级别的终端，定期对网络流量进行审视等。

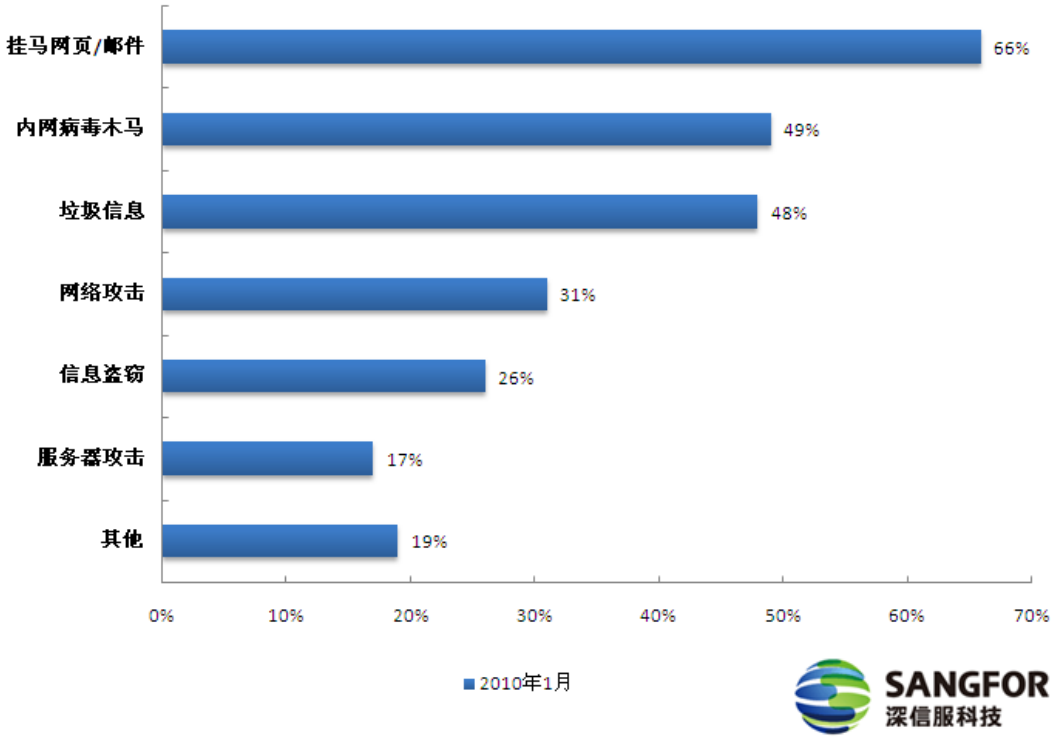


图 14:2010 企业网外部网络威胁组成排名

挂马网页/邮件：包括用户访问挂马、携带恶意插件、脚本的网页、邮件；

内网病毒木马：用户反馈终端通过网络（非 USB、蓝牙、红外等介质）感染病毒、木马的事件；

垃圾信息：垃圾邮件、垃圾广告网页、垃圾游戏网页；

网络攻击：端口扫描、DOS 攻击等，黑客攻击（将受害者的计算机纳入僵尸网络并利用以进行恶意活动）；

信息盗窃：因网络攻击引起的资料盗窃、个人信息泄露、账号盗用、账单篡改等；

服务器攻击：包括服务器注入式攻击、漏洞攻击、恶意广告插入、搜索引擎结果重定向、针对后端虚拟托管公司的攻击等等。

控制措施

“网络安全管理措施”内涵丰富，由于精力和篇幅的所限，本文我们通过“网络安全管理硬件部署情况”的对比来一探行业用户群体在过去一年中网络控制措施的变化。由于所选的样本用户网络建设相对完善，个别统计数据不一定适用中小规模网络。

两次调查的数据显示，传统的网络安全硬件如防火墙增幅最小，亮点集中在上网行为管理（增长 52 个百分点，含流量控制、应用行为记录产品、安全内容控制产品）、入侵防御（增长 30 个百分点）、统一威胁管理（增长 14 个百分点）、桌面管理（增长 19 个百分点）等。

解读：*不起眼的漏洞、随意的上网行为和过期的防护，合在一起会给 IT 管理造成极大困扰。IT 管理员深刻了解——仅仅依赖对用户进行教育并不足以提升效率、降低风险，组织应该制定明确的控制措施和安全策略，并采用能够保障这些策略执行的技术手段。同时，当今网络威胁越来越多的通过可信的媒介、可信的用户传播的，传统的基于边界的控制产品很难发现它们，IT 管理员需要获取关于流量与终端的信息，需要智能的可靠的方法来评估，并在任何异常的流量或存在安全隐患的终端引发问题前将其阻止。*

采用网络控制产品尤其是网络安全产品的组织大量增加，原因有两方面：

一方面受益于组织高层管理者的管理意识增强，我们曾多次听到 IT 管理员抱怨有决策权的高层管理者不重视，而有需求的中层执行者又无决策权，这种需求与决策脱离的情况随着高层管理者逐渐意识到投资 IT 对组织发展的价值而有所改善。

另一方面，随着网络应用的日益丰富与网络威胁的目的趋利化、手段更隐蔽，IT 管理员发现，在"风险评估"中分析的种种管理漏洞，单靠传统专注于 TCP/IP3 层、4 层的管理手段已不能有效解决，网络控制与安全管理的重点转移到以应用内容为主的 7 层上，在这一点上，上网行为管理等产品则表现突出。

随着科技的进步，未来将有更多的组织接受虚拟化这一概念，构建随时随地的协作办公，追求更高的生产效率和更低的成本。对于管理和安全的要求一直在提高，使得我们需要经常审视我们的控制措施。

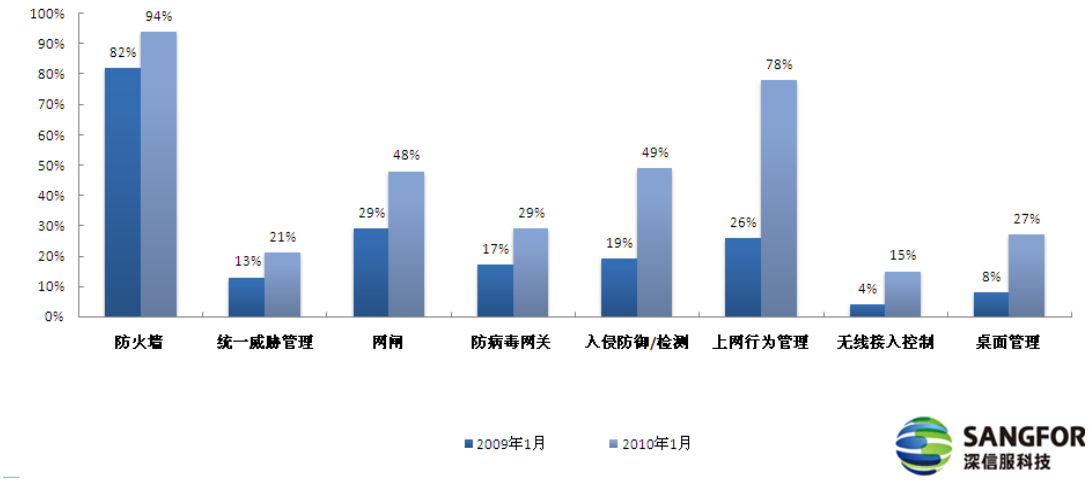


图 15：2009-2010 网络安全管理硬件部署情况对比

信息与沟通

本文第 7 页中，我们引用了 CNNIC《第 25 次中国互联网络发展状况统计报告》中“表 11 各类网络应用使用情况及用户增长”，信息获取类应用（搜索引擎、网络新闻）、交流沟通类应用（即使通讯、博客、论坛/BBS、电子邮件、社交网站）使用率高，而商务交易类应用（网上购物、网上支付、网银、在线炒股）增长速度较快。

信息需求直接拉动了信息获取与沟通类应用的增长，海量资源与更多途径在丰富了用户信息来源的同

时，也给 IT 管理员带来了困扰。

解读：*组织使用信息技术是为了确保合适的人使用合适的终端通过合法的线路获得适当的资源，并在这个过程中确保安全和高效。*

然而，随着网络的社交性增强，一方面，企业网用户将个人网络行为带入办公网络，业务通信和个人通信混杂交织，在信息交互与沟通之中，不知不觉地将业务运作的信息、个人的意见和行为传递出去，而 IT 管理员很难依靠防火墙等传统产品来判断这些行为中是否潜在诸如泄密、言论不当等风险；另一方面，用户对可信网络、可信用户高度信任，往往不假思索地接受来自此类途径的信息并作出积极回应，正因为如此，社交网络为不法分子实施欺骗提供了大量机会。近年来因为网络入侵导致的被动泄密，因为利益诱惑导致的主动泄密，舞弊事件等，已经给许多企业组织造成经济与声誉上的重大损失。

综上，在获取信息与保持沟通的过程中，管理者需要提前筛选、过滤不良内容，预防不当外发行为与言论，所以安全过滤、上网控制与行为记录方案获得管理者的认同和青睐。

监督与检查

2009 年，有 23%的组织坚持定期检查并输出检查报告，2010 年这一比例增加到 44%；更多的组织虽然没有将这一工作列入常规动作，但仍会不定期地进行抽查，或在特殊时期、网络异常、安全事件发生后、接到相关部门要求时进行检查。检查包括终端安全状况、网络行为监控、流量控制分析、异常流量与异常行为，检查结果往往通过对记录数据的统计、分析、对比并以报表形式输出。

解读：*管理措施都需要输出检查结果以验证效果、发现问题并调整改进，这是如今大部分 IT 管理员的共识。促成这种共识的原因有三个方面：第一，用户随意的上网行为、不到位的终端防护、泛滥的安全威胁给组织的 IT 管理造成极大麻烦。也给 IT 管理员带来大量的无谓工作，仅仅依赖对用户进行教育并不足以解决问题，对终端安全状况、用户网络行为、出口带宽使用情况进行定期的监督检查，才能及时发现问题，减少安全事故和管理压力；第二，过去，大多数网管部门只顾埋头干活，没有注意到定期检查并在工作汇报中体现监管效果，导致高层管理者对网络管理方面存在的问题关注不够，认识不深，而网络管理部门在提交建议以供高层做决策时又缺乏相关的事实依据，所提建议很难得到足够重视；第三，组织高层管理者通常都十分关注员工的工作效率，而员工的网上行为即与工作效率息息相关，监督检查机制可以让人力资源了解员工的网络工作效率。*

因此，组织需要监督检查机制来审核、评估控制措施的有效性，作为策略改进依据和考核依据，并为安全事件的发生做好应急预案。

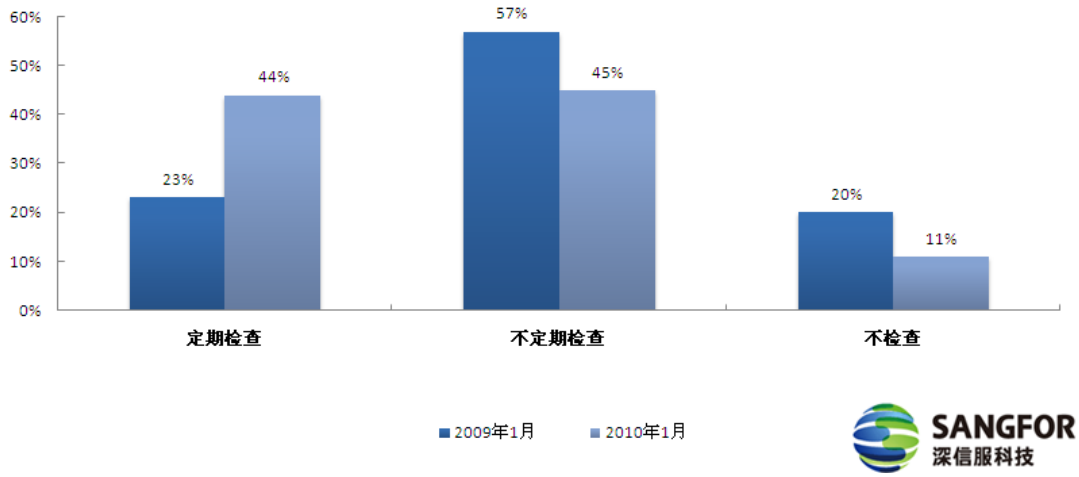


图 16：2009-2010 网络管理监督检查情况对比

国家政策要求

为了规范互联网环境，创造一个和谐的网络氛围，国家关于互联网管理的法律、法规、规范等陆续出台，其中典型的有：

- 《互联网安全保护技术措施规定》
- 《互联网信息服务管理办法》
- 《计算机信息网络国际互联网安全保护管理办法》
- 《中华人民共和国计算机信息系统安全保护条例》

  参见：http://baike.baidu.com/view/2821921.htm
- 《企业内部控制基本规范内控规范》

行业背景要求

- 金融：《银行业金融机构信息系统管理指引》、《金融机构保护用户信息法案》（GLBA）《支付卡行业数据安全标准》
- 政府：《中华人民共和国计算机信息系统安全保护条例》
- 电力：《电力二次系统安全防护规定》
- 教育：《全国青少年网络文明公约》
- 广电：《互联网视听节目服务管理规定》
- 运营商：《中国移动上网行为管理系统技术规范》

总结

本章节中，我们根据调查结果分析了现代企业网可能存在的风险及其根源，在此基础上，我们阐述了现阶段组织所采用的控制措施、在信息沟通中需要关注的安全、以及定期监督检查的必要性，并给出国家与行业监管部门的相关政策要求。无论是业务转型中自身发展的需要还是大背景的驱动，对网络行为进行风险分析、行为管控、信息过滤与信息安全防护、定期检查等都是大势所趋。然而，这些任务不是任何一款产品能独立完美完成的，组织需要不断创新的思路和寻找对应方案以完善、构建全局式的管理，我们将在下一章节中给出一些技术参考。

三、上网行为管理技术

前面，我们阐述了上网行为管理产品的需求来源、对企业网网络管理的现状进行了细致分析。本章节中，我们将介绍专业上网行为管理产品的核心技术和应具备的基础功能，以及在此基础上某些实力较强的厂商为用户提供的更多适应行业需求的高级功能。

核心价值

专业上网行为管理产品能为组织提供如下核心价值：

- 优化上网环境，提升用户用网体验；
- 优化带宽管理，保障核心业务、核心人员的访问速度；
- 管控网络应用，提高员工工作效率；
- 实现与职位相匹配的上网权限分配，防止越权访问；
- 防范信息泄露，保障组织信息安全；
- 过滤不良信息，规避由此带来的安全、管理与法律方面的问题；
- 修复安全短板，防止网络攻击，提升上网安全度；
- 支撑 IT 管理制度，优化组织 IT 管理环境；

核心技术

识别技术

识别是管理的基础，识别能力是评判一款上网行为管理产品专业度的重要标准。业内优秀的上网行为管理产品识别率普遍可以达到 85%~90%甚至更高。

- ***用户识别***

用户身份识别是实施管理的依据，主流上网行为管理产品所支持的用户识别技术包括本地认证、第三方认证、多因素认证、软件免认证、硬件免认证、单点登录技术、强制认证、临时用户、用户自注册等。

- ***终端安全识别***

终端识别技术包括终端硬件识别和终端安全状况识别等。终端硬件识别主要是资产管理系统的工作，我们不做过多关注。终端安全识别包括进程、注册表、操作系统与补丁、杀毒软件与病毒库升级、多网卡状态、应用程序检测等。

- ***应用识别***

上网行为管理产品的应用识别能力是重中之重，是产品发挥管理控制功能的根基。主流的识别技术有两种：DPI，也称“深度数据包检测”，即基于数据包组成内容特征的应用识别；DFI，也称“深度流特征

检测”，建立在应用特征的统计学规律基础上的行为识别，是具有智能特性的识别技术。

➢ ***智能识别***

✓ ***HTTPS 非法网站识别***

HTTPS 被广泛应用于通讯安全，如目前几乎 100%的金融类网站，部分门户网站均使用了 HTTPS 加密方式。大量钓鱼、挂马网站也使用 HTTPS 加密，而传统安全产品无法对 HTTPS 加密过的钓鱼、挂马网站进行识别，导致安全管理上存在严重漏洞。为解决此问题，部分上网行为管理产品提供了相应的 SSL 加密网站的甄别技术，将 HTTPS 类型非法网站排除在访问对象之外，保障网络安全。

✓ ***网页智能识别***

大中型上网行为管理厂商多数都有研发团队负责网页分类与 URL 库更新，以此作为网页过滤控制的依据。但是，2009 年“互联网网页数量达到 336 亿个，年增长率超过 100%”（CNNIC），靠人工手动分类的方式已远远跟不上网页的增长速度，加上大量的私博和社交网页并未被传统的 URL 库收归，导致即使这些网页存在问题也很难被发现。为此，技术领先的上网行为管理厂商提供基于关键字、基于网页分类特征的识别技术（如赌博类网站往往都有相似的关键字和结构），将人工分类的技巧“传授”给产品，让产品“学习”之后，将新访问的不在库中的网页自动分类入库。

✓ ***行为智能识别***

网络应用层出不穷，每天都有新软件、已有软件的新版本面世，尤其是 P2P 软件，仅靠已有的应用识别库来识别具有一定的滞后性。为此，上网行为管理产品应具备基于应用行为规律的智能识别技术，即便出现新的未知软件、未知版本，也能将其识别、管控。

➢ ***威胁识别***

来自网络的安全威胁如：带毒挂马的网页/邮件、黑客入侵、可信好友发来的潜在威胁的链接，来自组织内部的威胁：终端中毒发起攻击、异常外发流量、异常端口扫描行为等等，带来管理和安全问题。为此，威胁识别技术能及时发现、封锁、统计异常流量和异常终端，帮助组织提前规避风险。

流控技术

“基于 TCP 窗口整形的流控技术”和“基于队列的流控技术”是目前专业流控产品采用的较多两种技术。

➢ ***基于 TCP 窗口整形的流控技术***

基于 TCP 窗口整形的流控技术，通过调整 TCP 滑动窗口的大小来控制流量，该技术的优势在于控制尺度比较精确，但是采用此技术的产品往往性能有限（一般不能支撑超过 1G 的流量），一旦逼近极限就会出现较大误差。

➢ ***基于队列的流控技术***

顾名思义，“基于队列的流控技术”就是建立管道，将不同的控制对象分配到不同的管道里。该技术的好处是控制灵活，大通道中可以多层嵌套小管道，分别对应不同的用户、时间、应用协议、网站、文件类型等对象建立不同的通道，对于结构复杂又希望实现差异化控制的组织来说可以做到更为精确的控制。队列技术采用数据包调度，能实现了对大流量的很好的控制。

以一个实例来说明效果，假设我们要对一个出口带宽为 1G（由数条线路组成）的高校做带宽管理，产品以网桥模式部署：

- 物理线路->虚拟线路：桥模式下建立虚拟线路，可分别映射外网物理线路；
- 父通道->二级子通道->三级子通道

将出口 1000M 按规模划分给下属 3 个校区：300M、300M、400M；

其中，A 校区拥有 300M 出口，并为 A 校区设置分级 IT 管理员，允许根据校区内研究室、学院规模分配带宽；

- 子通道->虚拟子通道：每条通道可根据应用/文件/网站类型等进一步划分成虚拟通道；

A 校区 IT 管理员为某研究生实验室（30 人规模）分配带宽，将 4M 线路“动态”分配给上网用户（人数在 0~30 之间随意波动），并限定单用户下行不超过 200Kb，其中每个人的 P2P 下载不超过 50%，总线路的 P2P 应用不超过 30%。

云技术

在上网行为管理领域，“云技术”已得到应用，如通过互联网上已部署的产品发现、统计网络管理中出现的外来威胁、内在危险、未识别的流量/应用、行业应用特征、用户行为习惯等，基于“云”网络共享信息，为产品的优化改进提供依据，以便更好地提升用户体验。

基础功能

身份认证

基于身份认证技术，上网行为管理可以为组织提供多种身份认证方式，如：web 认证，与常见的第三方服务器结合认证（AD、LDAP、Radius、Rroxy、POP3 等），IP/MAC 绑定认证等，更高级的还有 key 认证、硬件认证等。部分厂商提供单点登录、用户自注册等，方便 IT 管理员使用。此外，为了符合公安部关于“互联网公共服务场所”的管理要求，有的产品提供了虚拟账号和真实账号的对应，如游戏账号、IM 账号、BBS 账号等。

身份认证功能帮助 IT 管理员建立网络用户管理体系，实现管理与用户的一一对应。

权限控制

提供基于时间、应用、用户（基本元素）的上网权限控制。权限控制功能帮助组织建立与组织文化、业务职能、用户职权相匹配的上网权限管理体系，防止越权访问，防范法律和泄密风险。

流量管理

提供基于时间、应用、用户组/用户、上下行带宽（基本元素）的流量控制，帮助用户限制与业务无关应用的带宽占用情况，保障核心用户、核心业务的带宽需求。识别率与流控粒度是评判产品优劣的重要标准。

应用行为记录

提供上网行为记录、数据挖掘、日志定位功能，一方面帮助组织提供满足主管部门要求的上网行为记录，避免安全事故发生后无据可查的情况，另一方面帮助组织进行业务分析，了解网络利用情况，应用行为记录功能也常常被作为信息安全防护、防泄密方案的重要组成部分。

安全防护

主流的专业上网行为管理产品都是硬件产品，作为管理产品其具有对网络威胁的识别和防御技术，一方面对网络威胁的防御（如防止 DOS 攻击、防 ARP 欺骗）能保护产品本身的稳定安全，进而保障网络可靠性；另一方面识别并拦截网络中的异常流量，可以避免威胁扩散而给组织造成不良影响。

高级功能

终端安全检测与修复

上文我们提到上网行为管理的“核心技术”之一“终端安全识别”包括进程、注册表、操作系统与补丁、杀毒软件与病毒库升级、多网卡状态、应用程序检测等等。但仅仅发现问题并不能满足 IT 管理员的需求。为此，部分上网行为管理厂商提供了扩展功能，支持和第三方的安全服务器结合，一旦发现存在安全隐患的终端，自动向终端发起提醒或主动运行相关程序，修复安全短板。

局域网准入控制

网络行为的管理不仅仅包括互联网行为的管理，也包括内网行为的管理。为此，部分上网行为管理厂商提供了局域网准入控制功能，依据对终端安全级别评估的结果，设立虚拟化的隔离区，将不同用户、不同安全级别的终端划入相应隔离区。IT 管理员可依据各隔离区的安全级别设置网络服务控制策略、分配互联网访问权限和与其他隔离区的通讯权限，拒绝安全级别较低的隔离区中的终端与正常通过安全策略检测的终端进行通讯。

虚拟化的多隔离区帮助 IT 管理员在终端识别的基础上有效区分对待安全级别不同的终端，避免存在安全隐患、不符合安全策略的终端随意接入内网，威胁其他用户，有效地遏制了病毒、蠕虫和间谍软件等损害网络安全。

服务器访问分析与控制

受“互联网应用分析与控制”的启发，许多组织将上网行为管理产品应用于业务流量分析与控制。据此，组织可以了解主页网站、电子商务网站的被访问情况，包括访问时间、次数、流量等，可以为服务器组进行带宽控制，避免访问流量过大影响其他用户的访问体验或影响服务器稳定。借助上网行为管理产品的报表，管理者可以导出自己需要的报表，据此做出更快更准确的决策。

免过度记录功能

许多组织在部署应用行为记录方案时都不可避免地遭遇来自各方面的管理阻力和舆论阻力，网络管理部门必须考虑包括“如何避免对关键人员（如组织高层领导）的过度记录”、“如何解决对日志的保护和保密工作”、“如何控制对日志的查看权限”等问题。

对此，大部分厂商都提供了基于软件的和对日志的软保护，但因为控制权在产品管理员手中，仍有高层管理者对此表示顾虑。部分厂商提供了更人性化的手段，使用硬件鉴权如 USB-key 的方式，免除对特定人员的行为记录，使用“key+密码”的方式限制对日志的查看权限，更进一步的，可以采用“两人分别持有 key 和密码，并且在第三者在场监督的情况下才允许查看日志”的方式，保障日志安全。

数据防泄密

由于认知程度的限制和侥幸心理的存在，在过去，数据防泄密管理方案的普及度十分有限。随着近几年各种数据泄密事件频频曝光，给个人或组织造成了声誉和财产上的损失，上网行为管理在数据防泄密方面的优势逐渐被重视起来：事前预防（过滤与控制技术、异常行为预警）、事发拦截（异常流量拦截、敏感内容过滤）、事后追踪（日志记录）。数据防泄密功能能帮助用户有效减少泄密风险。

四、未来的技术趋势和预测

适应性更强

支持 IPV6

IPV6 的产生最初是为解决 IPv4 定义的有限地址空间即将耗尽的问题，此外 IPv6 具有扩大地址空间、提高网络的整体吞吐量、改善服务质量(QoS)、更高的安全性、支持即插即用和移动性、更好实现多播功能等优势，IPV6 替代 IPV4 的尝试是当今的热门话题。因此，解决对 IPV6 网络的支持和管理是上网行为管理产品在未来几年必须考虑的问题。

移动互联网

据 CNNIC 调查显示，截至 2009 年底，中国手机网民规模年增加 1.2 亿，达到 2.33 亿人，占整体网民的 60.8%，增长率 98.3%，笔记本增长率 42.4%，互联网随身化、便携化的趋势进一步明显。上网门槛降低，无线上网突破时间空间限制的因素，3G 网络的开通使得上网速率提升等因素促使移动上网成为潮流。

对移动互联网的管理——包括对移动终端的识别管理、无线网络应用识别和带宽控制、行为记录等已经被各大运营商列入规划，上网行为管理如能满足移动互联网的管理需求，必将在这一领域大有作为。

识别率更高

三网合一

随着三网合一被提上日程，互联网应用从未像今日一样备受关注，对于应用的识别和管理的在相关部门的日程表中均占有重要的位置。为了有效提升识别率，“云”技术的使用是上网行为管理识别率的必经途径，“云”技术的使用让网络的共享不仅仅局限在数据的通讯中，也扩展到管理领域中。

管理更智能

与其他管理系统的结合

没有任何一个单一产品可以完美解决网络管理的所有问题，所以，网络产品总是在各自的发展中寻求与相关系统的结合之道。对于上网行为管理产品而言，与桌面管理系统、计费系统、身份认证系统、应用交付方案、应用性能管理系统进行有效联动，将为用户打造一个全方位、立体化的管理体系。

应用更安全

七层的安全

前面我们曾经提到，随着网络威胁更加趋利化、手段更隐蔽，靠传统的专注于 TCP/IP3 层、4 层的管理手段已不能有效解决，安全管理的重点正在转移到以应用内容为主的 7 层上。在这一点上，上网行为管理产品因其优越内容管理和识别能力，若能进一步加强安全防护功能，将有助于进一步提升上网安全性。

性能更强

性能为本

选购任何一台部署在网络中、对数据进行分析处理的产品，性能都是必须考虑的要素。随着各运营商之间的竞争，网络带宽势必越来越大，价钱越来越便宜，为了适应大带宽下的管理要求，在兼顾功能丰富与灵活性的基础上，上网行为管理产品的性能也将进一步提高。

附录

样板用户分析

《华东电网有限公司网络管理平台建设经验分享》

《上海文广新闻传媒集团内网管理分析》

《招商银行构建由内而外的安全管理机制》

《浙江吉利控股集团打好上市信息安全保卫战》

以上详情内容，请见蓝皮书附件。

网络管理指导书

深信服科技作为规模最大、创新能力最强的前沿网络产品供应商，于 2005 年推出国内第一台上网行为管理网关，并定义了上网行为管理产品的核心功能。多年来，深信服始终致力于帮助用户的业务向互联网转型，并在这一转型过程中获得成功与收益。

基于丰富的网络分析与管理顾问经验，深信服制定了本网络管理指导书，旨在为用户提供网络安全管理办法与技术建议，帮助用户制定适合组织文化与网络现状的 IT 管理制度，并采用相关技术手段保障制度的有效实施。

具体内容参见：http://www.sangfor.com.cn/topic/AC_program/index.html

产品选购指导

深信服建议，选购上网行为管理产品需要考虑多方面的因素，包含但不限于如下所列：

1.所选产品的性能不仅要满足组织现有网络规模，即产品性能对网络稳定性的影响，同时要满足组织未来三到五年的扩容规划；

2.所选产品能解决组织现有问题，对网络应用现状有何改善，有助于业务开展；

3.产品在同行业用户中的应用口碑，即厂商的同行业用户案例是否足够多、足够有代表意义，该项有助于降低采购风险；

4.产品/方案的灵活性要能满足组织文化需求，能兼顾人性化和信息安全防护（如在满足公安部等相关部门对上网日志的要求的同时，能否兼顾日志安全防护）,该项有助于降低管理阻力；

5. 厂商的售后服务能力要有保障，如在各地均有厂商直属办事处，响应及时、提供备机备件服务等均要列入考虑范围。特别是对全国部署的项目，厂商售后服务能力尤其重要。

除此之外，采购时还需要考虑方案的可扩展性、性价比，以及厂商在项目管理方面的经验，能否根据行业需求适时提出管理建议等等。

免责声明

深信服科技声明：本蓝皮书所有数据统计结果均来自深信服科技选取的 100 个典型样板用户实际报表。本皮书谨供媒体、公众和相关政府及行业机构、厂商作为上网行为管理市场、技术、趋势预测等信息的介绍和研究资料，使用本皮书中的任意文字或图表请注明出处。由于客户样板选取标准的针对性，报告中数据结果可能与其他调研数据有所偏差，如若蓝皮书阐述之状况、数据与其它机构研究结果有差异，请使用方自行辨别，深信服科技不承担与此相关的一切法律责任。