深信服上网行为管理

——让上网可视可控、让数据更有价值

SANGFOR Internet Access Management

www.sangfor.com.cn

SANGFOR
深信服科技

深圳市南山区学苑大道1001号南山智园A1栋
市场咨询热线：400-806-6868　服务热线：400-630-6430
邮编：518055　邮箱：market@sangfor.com.cn

深信服官方微信

深信服手机二维码

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

深信服上网行为管理

01 产品概述

深信服上网行为管理连续9年市场占有率第一（数据来源 IDC），它一直秉持“让上网可视可控，让数据更有价值”的理念，通过专业的用户认证与管理、应用控制、流量管控、信息资产防护、非法热点管控、大数据日志分析等功能，让客户看得清带宽流量现状，管得住应用和内容，以此提高办公效率、规避泄密和法规风险、保障内网数据安全、实现可视化管理，同时让数据更有价值。

深信服上网行为管理广泛应用于政府、教育、金融、企业等办公网互联网出口（千兆和万兆）、有线无线混合网络出口、多分支组网、多门店无线增值营销、内网用户认证等场景，目前服务于 2 万多家各行业用户。

02 中国上网行为管理优质品牌

市场第一

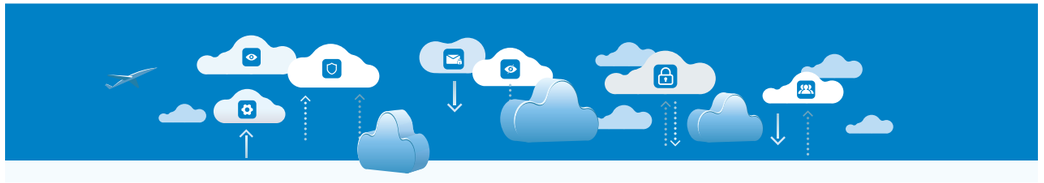
- 连续 9 年中国市场排名第一
- 2015 年市场占有率 36%，超第 2、第 3 和第 4 名的总和（IDC：2015 下半年中国安全硬件市场分析报告）
- 中国入围 Gartner SWG 魔力象限的产品，并且连续 5 年成功入围

前沿技术

- 更早推出有线无线网络统一上网行为管理解决方案
- 拥有全国更大的应用识别特征库和 URL 库
- 获得 25 项产品技术专利和 30 多项媒体奖项
- 率先通过国家信息安全产品 EAL3高等级认证
- 率先获得 IPv6 Ready 认证的上网行为管理产品

用户认可

- 20000 多家全国各行业用户
- 80% 世界 500 强的中国企业
- 60 多个政府细分行业（最高人民检察院、外交部、公安部等）
- 40 多个省级运营商用户
- 32 个省级电子政务外网，地市区县覆盖率达 70% 以上
- 430 家金融行业客户（中农工建交五大行，招商、兴业、民生等 12 家股份制银行）
- 服务于 G20 杭州峰会、世界互联网大会、奥运会、世博会、亚运会、青奥会等大型活动



PART 1 让上网可视可控

01 为什么上网需要可视可控?

“看不见管不住”让网络管理更困难

互联网已经成为重要的生产资料，越来越多组织的业务在向互联网迁移，然而互联网却是一把“双刃剑”，管理得好可以让办公效率大增，促进业务的发展；而缺乏管理的互联网将带来诸多问题，不仅降低工作效率，还给组织带来各种业务风险。

非法、难定义的上网行为，给客户带来各种问题

办公效率低下：

员工在上班时间玩游戏、聊天、看视频、浏览新闻、在线购物等；

企业信息存在安全风险：

各种外发途径（如 HTTP 上传、网盘上传、论坛发帖和上传、邮件外发附件、IM 外发、微博上传等）容易泄露企业核心信息，造成无法估量的损失；

无线网络缺乏有效管理：

在有线和无线混合使用的网络里，有线和无线网络无法统一管控，移动 APP 应用无法有效识别和控制，无线用户权限无法精细划分，管理难度大。

核心业务无法保障：

员工大量进行 P2P 下载、在线视频等带宽占用大的应用，容易挤占正常业务系统带宽（如 OA 系统、邮件系统等），影响核心业务的正常进行；

非法 Wi-Fi 热点暴露内网：

无线共享工具如 360 随身 Wi-Fi、小度 Wi-Fi、小米 Wi-Fi、猎豹免费 Wi-Fi 软件等，价格低廉且易用，此类共享网络的行为容易导致内网暴露，成为不法分子入侵内网的跳板，窃取核心资料或攻击内网，造成极大的安全隐患；

02 实现上网可视可控的本质

造成上述网络管理问题的各类上网行为，从逻辑上可以分为用户、终端、应用、内容、流量 5 个要素，而从业务管理的角度可以合并为“用户和终端”、“应用和内容”、“流量”三个元素。因此，要解决上述问题，即要实现上网的可视可控，就是要实现“用户和终端”、“应用和内容”以及“流量”的可视与可控。

03 实现上网可视可控存在诸多挑战

互联网上各种应用快速更新跌代，新应用、新场景也层出不穷，网络中不断进行着识别、管控、隐藏、再识别、再管控、再隐藏……这样的对抗循环。当前，要实现网络的可视、可控，存在着诸多的挑战：

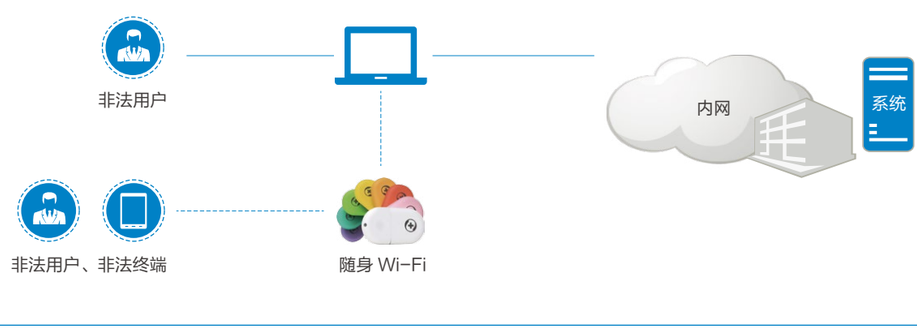
◎ **互联网创新不断，导致可视与可控不断的被挑战**

互联网新应用层出不穷
移动互联网和无线让环境更加复杂
各类新技术让应用的识别与管控更困难

用户和终端方面

挑战：非法用户和终端通过非法方式接入内网

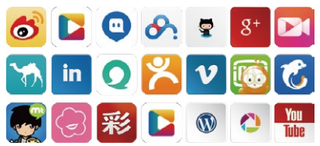
一些非法用户和终端采用非法的方式接入内网（如：随身 Wi-Fi、家用无线路由器等），这些无线共享工具将组织内网暴露在无线中，容易被不法分子入侵，一旦被侵入内网，不法分子可窃取内部核心资料，甚至破坏内部网络，造成网络瘫痪。



应用和内容方面

挑战：层出不穷的应用让网络难管理、难运维

大量新应用和老应用的新版本，给应用识别与管控以及后续的运维带来巨大的挑战，让网络难管控，难运维。



◎ 每天有几十种新应用推出

据不完全统计，仅 PC 应用每天就有几十种新应用上线。

版本号	主要更新内容	发布时间	迭代周期(天)
1.0	1、文字消息 2、图片分享 3、设置个性化头像	2011.01.21	
1.1	1、与微博私信互通（插件） 2、好友备注 1、群聊	2011.03.10	20
1.2	2、公司邮箱找人 3、黑名单 1、支持插入表情	2011.03.21	11
1.3	2、好友搜索 3、邀请好友	2011.04.06	16

◎ 每半个月更新迭代一个新版本

大量应用快速迭代版本，几乎半个月推出一个新版本（如微信前期平均 15 天发布一个新版本）

挑战：同一个应用的“好功能”和“坏功能”，管和不管两难

另外，即使是同一个应用也可能具有两面性，他们有“好”的功能，也可能有“坏”的功能，“好”功能具有实用性，而“坏”功能具有风险性，因此，此类应用的管控成了一个两难的问题。

▶ **同一个应用有两面性**

好功能具有实用性：如网盘下载、论坛浏览等知识查询功能
坏功能具有风险性：如网盘上传、论坛上传附件等存在泄密风险

▶ **“管”和“不管”两难**

管：正常业务需要下载和浏览相关内容
不管：一旦外发了内部核心文档，将造成巨大损失

挑战：先进的加密和隐藏技术让非法内容轻松绕过监管

据 Gartner 分析，超过 50% 的国外网站已经采用 SSL 加密方式，而国内 HTTPS 网站数量也在快速增长，而且越是非法网站，越会采用加密的方式隐藏其内容。因此，趋近 50% 的网站内容将不可控。

不仅如此，Gmail、163 Mail、QQ Mail 等主流邮箱已经默认采用 SSL 加密方式传输，这些主流加密邮箱将会成为泄密的重灾区。而流行的自由门、无界等代理软件，能够轻松绕过组织的监管，让网络管理和网络安全形同虚设。

因此，先进的加密、隐藏技术让非法内容绕过监管，成为实现应用和内容可视可控的重要挑战。

▶ **流量方面**

挑战：识不全、管不住的无关流量影响网络可用性

由于 P2P 流量没有明显的协议特征，再加上其带宽侵蚀性的特性，造成 P2P 流量的全流量识别困难。大量客户反馈已经有传统流控设备，业务却依然卡顿，也是这个原因。通过测试传统的流控设备，我们发现 P2P 应用的流量识别率只有 40% 左右。因此，60% 的 P2P 流量无法识别，而这 60% 看不见、管不住的 P2P 流量将直接抢占业务带宽，影响核心业务正常的运行，这将成为实现流量可视、可控的巨大挑战。

◎ **60%的P2P流量无法识别出来**

- P2P 应用链接多
- P2P 流量没有明显的协议特征

传统流控技术已经失效：

传统行为管理设备对 P2P 流量的识别率：

应用名称	传统行为管理设备统计结果【单位 M】	实际流量	识别率
ppstream	9M	20.7M	43.48%
PPTV	9M	21.9M	41.10%
QQ 旋风下载	9M	20.3M	44.33%

04 如何实现上网可视可控?

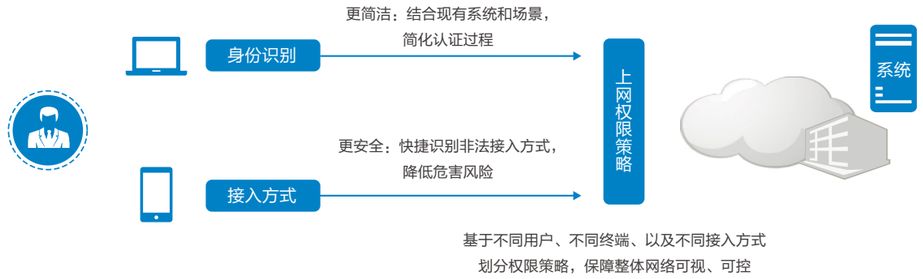
▶ **深信服一直为实现上网可视可控而不断创新**

不管在过去的互联网时代、现在的移动互联网时代，还是即将到来的云和大数据时代，深信服一直致力于实现上网的可视可控，并不断为之创新：

	用户和终端	应用和内容	流　量
云和大数据时代（分布式、海量数据）	**云化AC方案：**保障业务在云上可视可控 **开放大数据平台：**让海量数据为用户创造无限业务价值		
移动互联网时代（移动、无线技术）	**移动终端多场景身份认证** 基于场景的认证方式 非法 Wi-Fi 热点管控 基于终端类型和位置策略	**移动应用与细粒度管控** 移动应用识别 应用细分控制 应用标签化	**更人性化：兼顾管控与体验** P2P 智能识别 动态流控 流控黑名单
互联网时代（PC、有线网络）	**PC的准确识别与控制** 账号密码、IP/MAC 绑定与 AD 域等认证系统结合 防共享上网 基于组织机构的权限策略	**全面识别与控制** 千万级 URL 库 应用识别库 加密网页 / 邮件过滤审计 代理应用 ĸ　识别管控	**准确识别与控制** 各种应用流量准确识别 基于特征 P2P 流量 八级父子通道 基于应用的流量策略

▶ **如何实现“用户和终端”的可视与可控?**

为客户提供更简便的身份识别和更安全的接入方式之外，基于不同的用户、终端及接入方式划分权限策略，实现“用户和终端”的可视与可控。



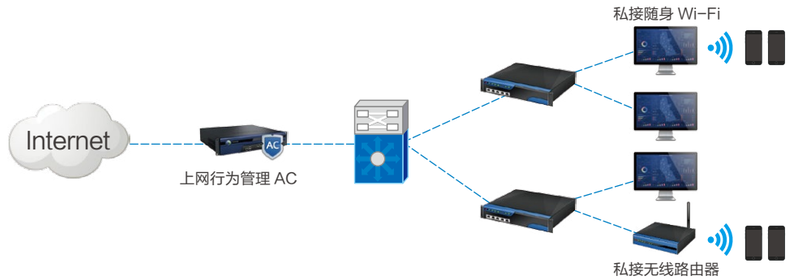
技术1：结合业务场景和现有系统，认证更灵活

上网行为管理的身份识别系统不但考虑客户不同的业务场景，除了普通办公的账号密码认证之外，还有面向公共区域顾客的无线上网，兼顾简单、安全和增值的需求；另一方面，我们能够无缝对接客户环境中现有的用户管理系统，比如能够结合 AD 域、Radius、城市热点等，尽量降低客户网络的复杂度，降低客户实施和运维的难度。

结合业务场景	结合现有系统
账号密码认证： 正常办公认证 短信认证： 手机号增值营销 二维码认证： 访客简易认证	AD 域 Radius 认证服务器 城市热点 SAM CAMS POP3 系统 各种类型数据库

技术2：非法接入管控技术，让非法接入无处藏身

无线共享网络的行为，是内网安全的巨大隐患，上网行为管理产品需要能够准确的识别无线共享行为，秒级发现，立刻封堵，并迅速告警。



▶ 如何实现“应用和内容”的可视与可控?

深信服通过四个步骤来实现“应用和内容”的可视可控: 首先全面 K　识别应用，然后基于业务视角管控应用，其次更细粒度的管控应用，最后对于特殊应用内容进行定向 K　识别与管控。

全面准确识别应用	业务角度管控应用	更细粒度的管控	防止非法内容绕过监管
• 完善的 URL 库 • 全面应用特征识别库 • 持续快速的更新迭代	• 应用业务属性标签 – 降低工作效率类 – 高带宽消耗类 – 高泄密风险类 – 安全风险类	• 识别应用的细分功能 – 封堵风险动作 – 放通实用动作	• 代理软件 （自由门、无界等） • SSL 加密 （加密网页、邮件等）
识别和管控应用	业务角度管控应用	更细致的管控应用	特殊应用内容控制

技术1：完善的应用识别技术，覆盖99%以上的常用网站和应用

凭借十五年应用层技术积累，深信服力争将每个应用的识别做到更好。截止目前已经积累了几千万条分类 URL，以及 6300 多条规则，2800 多种应用，1000 多种常用移动应用 APP。而且，深信服保持每半个月更新一次的快速迭代，不仅新增常用应用，还及时淘汰老旧应用，避免识别库的臃肿。

全面准确识别常用应用和网站

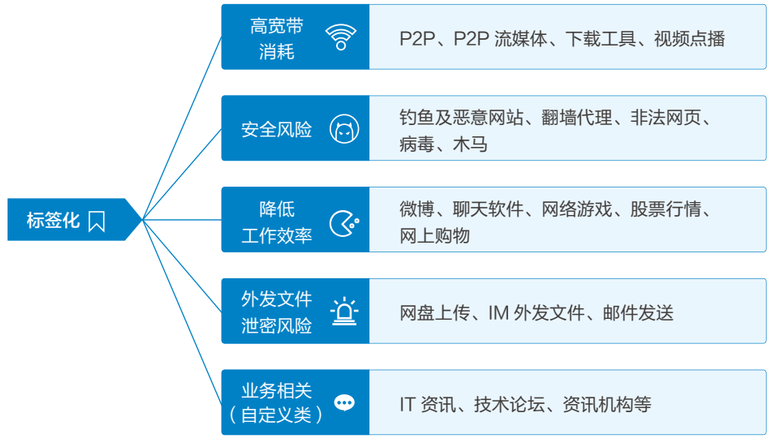
2800+ 种应用
1000+ 种移动应用
千万级 URL 分类库

快速更新及时淘汰，时效性更强

每两周更新一次
老旧应用及时淘汰

技术2：业务角度管控应用，一切以业务价值为中心

从业务角度对应用进行标签化分类，更好的对应用进行管理和分析，让业务高效、稳定。同时，由于应用数量众多，容易错配漏配，标签化能让应用管理更准确、简单，更易运维。



技术3：精细管控应用的细分功能，兼顾安全和实用性

针对具有多面性的应用，比如网盘，其上传功能有泄密风险，而其下载具有实用性，因此，应该精细管控网盘的不同动作，如：封堵网盘上传，放通网盘下载。通过精细化的管控，兼顾安全和实用性。

区分功能

论坛微博等应用，区分登录、浏览、发帖、上传附件等动作，如可浏览论坛，但禁止发帖，降低违法风险。

区分方向

华为网盘、360 网盘等，区分资料上传、下载等方向，防止机密数据泄密。

技术4：强大的SSL内容识别与代理识别技术，防止非法内容绕过监管

深信服通过专利技术，准确识别 SSL 加密的网页和邮箱等，并能够对加密内容进行有效过滤，同时，依托多年应用层技术积累，深信服的代理识别技术能够识别包括自由门、无界在内的 40 多种代理软件，通过对这些非法内容的识别，能够有效的防止非法内容绕过组织监管，保护上网内容安全，真正做到应用和内容的可视与可控。

▶ 如何实现“流量”的可视与可控?

深信服流量控制的目标是更全更准的管控与更人性化的管理。管控方面，主要是对 P2P 应用的全流量管控，以及基于用户、终端等多维度应用流量统计；管理方面，主要是从单级策略到多级策略，从静态策略到动态策略，从一刀切的封堵，到疏堵结合的方式，多种创新技术结合，既能保障业务正常高效的运行，还能兼顾用户体验。

流量识别更全、更准

◎ **应用识别全面，尤其是 P2P 应用**

全流量识别 P2P 流量、准确的控制 P2P 下行流量

◎ **多种维度流量统计**

基于用户、终端类型、文件类型、时间等

更人性化的流量管控策略

◎ **从单级策略到多级策略，策略制定更加灵活**

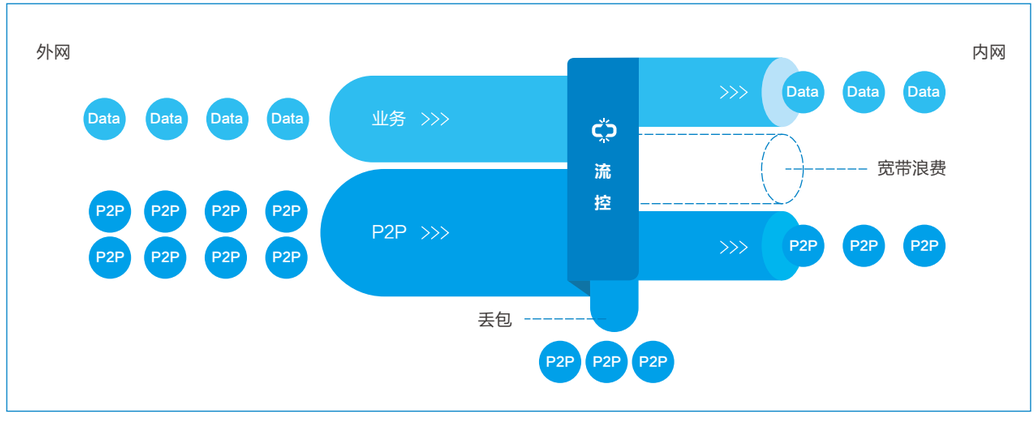
◎ **从静态策略到动态策略，用户体验更大化**

◎ **从一刀切封堵到疏堵结合，兼顾业务和体验**

技术1：准确控制P2P上下行流量，实现业务带宽有效扩展

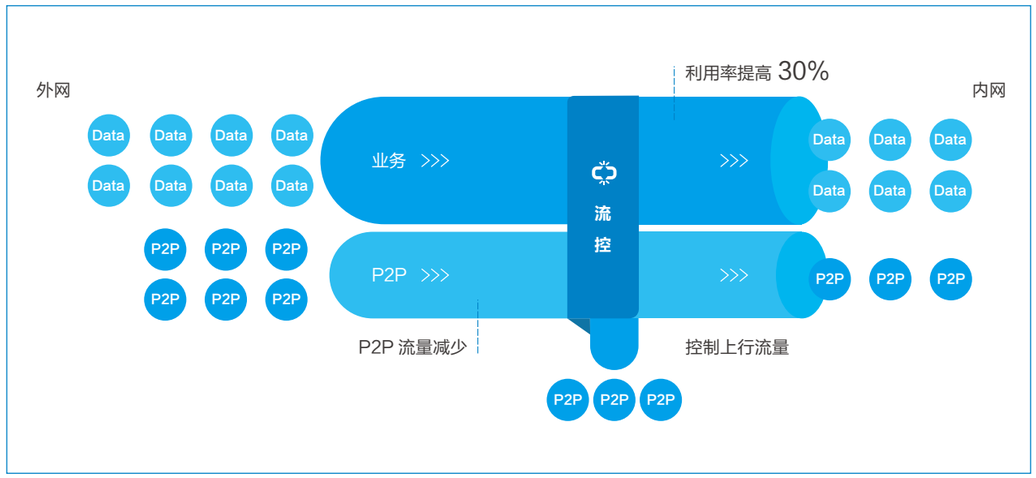
◎ **传统流控设备治标不治本**

传统流控基于缓存丢包的技术，但由于 P2P 应用的带宽侵蚀性，导致即使流控设备保障了内部 LAN 网口的带宽空余，但实际上，流控设备的 WAN 口依然被大量的 P2P 下行报文占满，最终实际业务带宽无法得到有效扩展。



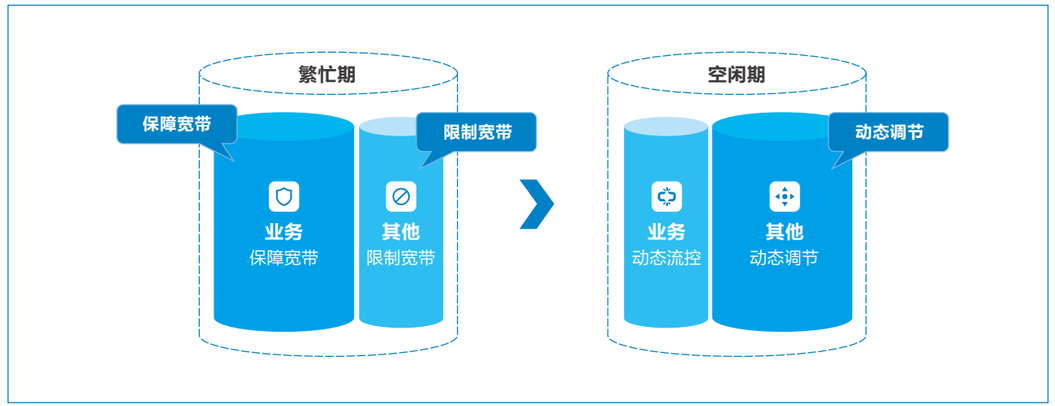
◎ **P2P 智能流控技术，真正扩展业务带宽**

深信服 P2P 智能流控技术，通过抑制 P2P 上行流量，达到降低 P2P 下行流量的目的，使流控设备的 LAN 口和 WAN 口的 P2P 流量一致，真正让业务带宽得到有效扩展，使得整体带宽利用率提高 30% 以上。



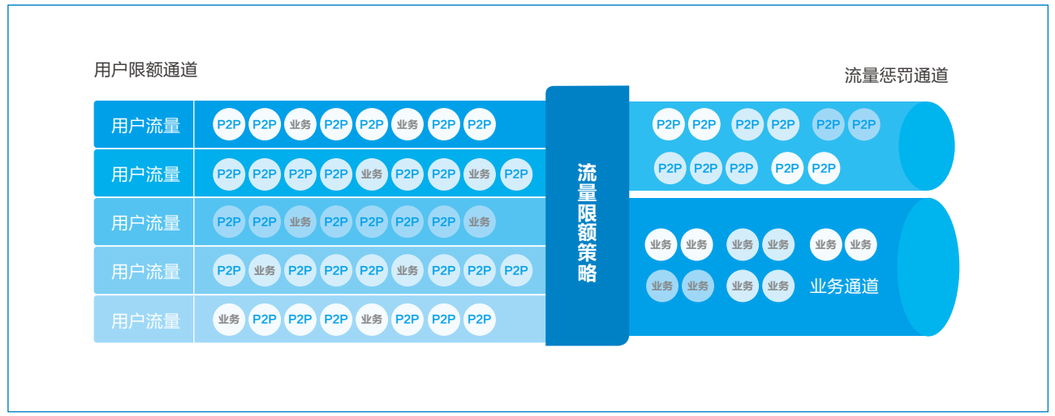
技术2：动态流控，空闲时突破限制，带宽利用率提高15%

组织管理员往往既希望在网络应用高峰期保障核心用户、核心业务带宽，限制无关应用占用资源，又希望在带宽空闲时实现资源的充分利用。为此，深信服 AC 支持用户间带宽的“自由竞争”与“动态分配”，除了基于父子通道进行流量控制之外，还可以根据整体带宽的利用率进行动态调整，上浮“限制通道”的更大带宽值，避免带宽浪费，提高带宽利用率 15% 以上。



技术3：疏堵结合，兼顾业务保障和用户体验

当用户的配额超限的时候，传统流控设备会直接封堵用户所有流量，这种一刀切的封堵，不仅影响了业务开展，同时还影响了该员工的用户体验。深信服流控黑名单技术，针对超额的用户，将该用户非业务应用的流量（P2P 流量等）引入惩罚通道，降低此类应用的流量。而该用户的正常业务流量仍然在业务保障通道中，不受影响。这种疏堵结合的流控方式，兼顾业务和用户体验，有助于减少内部投诉，缓和部门间矛盾。



PART 2 让数据更有价值

01 为什么要让数据更有价值?

大数据时代，数据将成为变革的驱动力

麦肯锡：

“数据，已经渗透到当今每一个行业和业务职能领域，成为重要的生产因素。人们对于海量数据的挖掘和运用，预示着新一波生产率增长和消费者盈余浪潮的到来。”

“大数据时代预言家”维克托 · 迈尔 – 舍恩伯格：

在其《大数据时代》一书中提到“大数据开启了一次重大的时代转型，大数据将带来巨大的变革，改变我们的生活、工作和思维方式，改变我们的商业模式，影响我们的经济、政治、科技和社会等各个层面。”

海量上网行为日志蕴含无限价值等待去挖掘

一个 200 人的公司每月会有 240G 上网行为数据
一个 500 人的公司每月会有 600G 上网行为数据
一个 20000 人的公司，一个月大约会有 60T 的上网行为数据

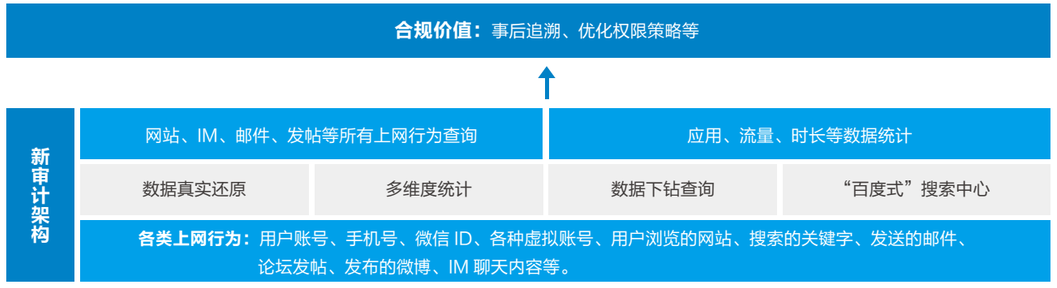
上网行为日志包含的信息量巨大：

用户身份、手机号、微信 ID 等各种虚拟账号，同时还包括用户访问的网站、搜索的关键字、发送的邮件、访问的论坛、发布的微博等所有上网行为产生的日志

02 如何让数据更有价值?

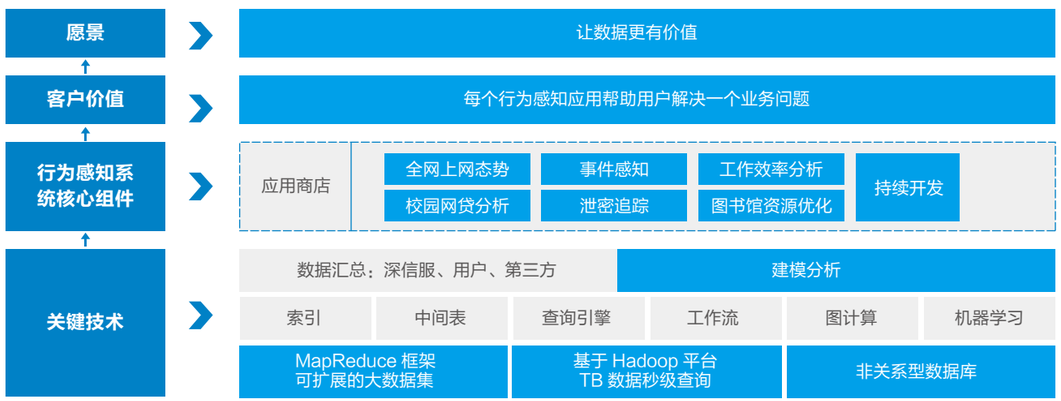
过去，提供完善的合规价值

过去深信服基于各类上网原始数据，通过多种创新的技术，如多维度统计、下钻查询、百度式搜索中心等，为用户提供行为查询与数据统计两大类报表，以此来满足事后追溯和策略优化等合规价值，得到了众多客户的称赞。



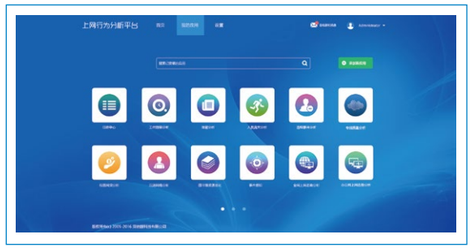
现在，提供专业的行为感知系统

数据价值的挖掘，必然依赖于海量的原始数据，然而，并不是拥有海量数据就可以挖掘价值，必须要有先进的技术支撑，才能够完成大数据的价值挖掘。深信服采用基于 MapReduce 框架的可扩展大数据集模型，以及自主开发的非关系型数据库，承载海量的上网原始数据，形成基于 Hadoop 的行为感知系统。



03 行为感知应用商店

深信服行为感知应用商店，基于上网行为管理日志中心平台，所有的日志分析应用以 APP 的形式发布到应用商店中，APP 形式的好处是与上网行为管理的软件版本解耦和，可以做到随需索取，用完即走，就像我们在 PC 上安装播放器、浏览器一样简单。



应用一：全网上网态势分析

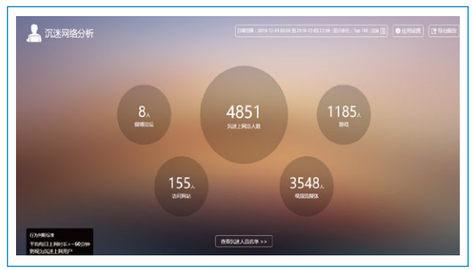
整体把握广域网各分支上网现状以及安全现状，及时发现管理和安全的薄弱点，便于制定有效的处置策略。

应用二：校园网贷分析

帮助学校及时发现高危网贷学生，提供及时准确的沟通辅导对象，防止不良后果发生。

应用三：沉迷网络分析

帮助学校发现沉迷网络的学生，便于进行有针对性的辅导和教育，拯救更多被网络毒害的学生



应用四：图书馆资源优化

帮助学校分析已购买和未购买的资源，为图书馆资源优化提供数据支撑。

应用五：事件感知

帮助组织及时发现内部特殊的恶性事件，为事件的妥善处置创造更多的时间，避免发生难以控制的负面影响

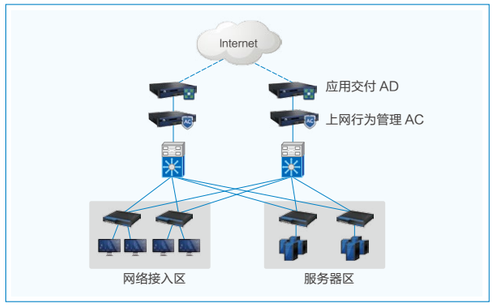
PART 3　典型方案

01　互联网出口上网行为管理解决方案

随着信息技术的发展，政府、企业等单位的业务模式在不断发生改变。有许多重要的业务是通过互联网来进行，如果对公司网络没有有效管理，过度开放的网络环境必会带来种种问题：大量与业务无关的网络应用耗费时间，降低员工工作效率；P2P 等高带宽消耗类型应用占用大量带宽资源，严重影响业务正常进行；员工肆意外发非法言论，组织承担法律责任。

因此，各组织需要针对互联网出口进行上网行为管理：

- 全面的应用控制：在上班时间合理管控与业务无关的网络应用，提高工作效率；
- 有效的流量控制：合理分配带宽资源，保证业务带宽，提高带宽利用率；
- 对于有信息溯源需求的用户：详细记录内网人员上网轨迹作为追查依据，满足国家合规要求；
- 组织分支机构一体化网关：由总部集中管理平台统一管控，管理更高效可靠。



部分成功案例：

政　府：中华人民共和国外交部 、中华人民共和国公安部、中共中央党校
教　育：中国人民大学、中国政法大学、中南大学、电子科技大学
金　融：中农工建交五大行、招商银行、中国银联、中国人寿、太平洋保险
运营商：中国移动、中国电信、中国联通、中国广电
能　源：中国国电集团公司、中石化国际石油勘探开发公司、国家电网、冀中能源
大企业：中铁十三局、中国一汽、宝钢集团、马鞍山钢铁、南方航空、北京王府井百货、中兴通讯、科大讯飞、创维数字、新浪、小米、当当。

02　万兆上网行为管理解决方案

以太网技术不断发展，网络带宽从十兆、百兆、千兆到万兆不断演进，用户对设备的性能以及带宽要求不断提高；全球 IPv4 地址已耗竭，IPv6 时代即将到来，在运营商和教育行业中已率先启动 IPv6 应用业务，其他行业也正处于过渡阶段，可以预见，在未来几年中 IPv6 将是 IT 科技行业里的主旋律。

深信服万兆上网行为管理解决方案：

- 采用全新高性能硬件平台，单向处理性能超过 10G，满足用户对设备高性能、高稳定性的需求；
- 支持 IPv6，对协议支持进行了优化，在混合协议的情况下，能承载更多的流量，帮助用户平滑过渡、节省网络设备投资。

部分成功案例：

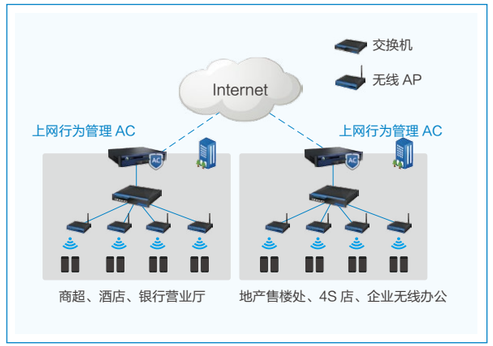
国家电网公司，国家税务总局，一汽集团，中国电信重庆分公司，中国联通河北分公司，北京外国语大学，农科院研究生院，辽宁省图书馆，广州电信，湖北广电（视讯），承德移动，顺义政府信息中心。

03　公共Wi-Fi上网管控解决方案

在机场、酒店、商场、银行营业厅、售楼部等公共场所普遍部署了无线 Wi-Fi，人们通过移动终端就能随时随地接入互联网。对于开放的网络环境，不仅需要提供高效快捷的网络接入方式，还要提供良好的使用体验。同时互联网中具有大量的反动、色情、赌博等不良网站，如果用户登录访问并发布非法言论将带来违法风险，因此这些无线上网行为需要得到合理管控。此外，移动用户数量庞大，网络运维过程中会出现大量日志数据，如何从中挖掘有效信息以及进行业务增值也是一个需要解决的问题。

深信服公共Wi-Fi上网管控解决方案：

- 通过微信认证，有效帮助企业公众号拉粉，聚拢核心用户群体;
- 支持短信认证，简单获取用户信息，作为后续定向营销的有效途径；
- 多种方式的广告推送，让用户实时了解最新动态；
- 用户数据分析，丰富的日志报表为企业提供决策依据；
- 支持与网监平台对接，满足监管机构的审计要求，让上网依法合规；
- 主动过滤反动、色情、赌博等不良网站，规范顾客的上网行为，规避法律风险；



部分成功案例：

合肥百货大楼集团，王府井百货，嘉禾影城，华强广场，SOHO 中国，凯德商场，华夏幸福基金，朝阳大悦城商场，赫基国际，世贸君澜酒店集团，华润万象城，厦门航空（酒店）

04　行为感知方案

大部分客户的上网行为管理设备都记录了大量用户上网日志，主要用于事后追溯，满足合规。而实际上，海量的上网日志中蕴含着大量信息，这些信息一直处于沉睡状态，无法得到有效利用。同时，由于互联网信息化的高速发展，网络已经融入社会生活的方方面面，许多组织问题和业务问题都和上网有所联系，比如学生沉迷网络、员工上班购物聊天、恶性事件传播、员工离职等。

其实，通过分析上网数据，可以很好的帮助客户有效应对这些问题。深信服行为感知方案，帮助客户挖掘数据价值：

- 采用完全自主的可扩展大数据分析架构，TB 级数据能够秒级查询分析；
- 基于不同行业客户的业务需求，不断推出有针对性的数据分析应用，真正给客户带来有用的数据价值，如：全网上网态势分析应用、校园网贷分析应用、泄密追踪应用、工作效率分析应用等；
- 各个数据分析应用相互独立，在行为感知应用商店中统一管理，客户可以随取所需，简单易用。

部分成功案例：

江苏武警总队、沈阳经信委、上海虹口教育局、广州南沙教育局、溧阳教育局、重庆广播电视大学、安徽工商学院、新疆喀什大学

05 有线无线统一管控解决方案

无线网络迅猛发展，大多数企业单位都在组织内部部署了无线，有线办公正逐步向无线办公转变，智能移动终端也超过 PC 成为常用终端。但同时，移动应用多种多样，大量与工作无关的应用既占用带宽又占用员工上班时间，需要进行有效管控。而且如随身 Wi-Fi 等无线私接设备普遍存在安全隐患，不但占用网络资源，而且易造成管理漏洞。因此，如何同时管理好有线网路和无线网络成为 IT 部门重点关注的问题。

深信服有线无线统一上网行为管理解决方案

- 同时管理有线网络、无线网络，同时管理移动终端、PC/ 笔记本，管理无漏洞；
- 能够对 900 多种移动应用进行有效地识别和精细管控（如微信传文件、微信聊天、微信朋友圈、微信游戏）；
- 能够基于位置、应用、终端、用户四维一体的识别与权限控制；
- 对非法无线热点能够及时发现和准确控制，秒级识别非法热点；
- 具备业界先进的内容识别与管控技术，可以对多种外发途径的数据进行有效管控；
- P2P 智能流控技术、动态流控技术，流量管理更 к 、更灵活。

部分成功案例：

湖北省统计局、温州国税局、中南大学、电子科技大学、招商银行、中信证券、中铁四局、上海医药、王府井百货、顺丰速运。

PART 4 典型案例

国家互联网信息办公室

国家互联网信息办公室是经国务院批准设立的互联网信息监管机构，致力于推动我国互联网持续繁荣发展，其日常工作大都与互联网业务相关。国家网信办通过深信服上网行为管理解决方案，精细管控各类应用流量，减少无关应用的带宽占比，提升数据信息交互速度，为互联网信息监管等核心业务保驾护航。

中国科学院

中国科学院作为国家科学技术方面高等学术机构，拥有大量的珍贵资料。通过部署深信服上网行为管理解决方案，中国科学院在总院和多个分院间建立了安全传输网络，管理人员可以对各种网络行为，包括 IPv6 应用，进行精细化的监管，减少无关流量对带宽的占用，提升应用访问速度，为科研项目的顺利开展提供了信息安全保障。

上海虹口教育局

上海虹口教育局在教育城域网建设到一定阶段后，发现无法全局掌握各中小学出口上网和安全现状，无法统一管理所有用户和上网权限策略，因此在所辖所有中小学出口部署上网行为管理（AC）和下一代防火墙（NGAF）设备，同时在教育局部署行为感知系统与所有 AC 和 NGAF 对接，同步和展示教育城域网各学校的管理和安全信息，让全网信息一目了然，便于统一监管。

招商银行股份有限公司

招商银行深圳总行以及全国共计 40 余家分行均部署深信服上网行为管理解决方案，全行 40,000 余人通过此网络线路开展工作，上网行为责任到人；P2P 流量得到有效控制，不再出现业务带宽被无效流量占用的现象；内网安全得到全面提升，终端安全得到加强；外发信息管控，有效避免内网敏感信息外泄的可能。数据信息的高效交互，提升了业务开展效率。

新浪集团

新浪及其子公司现在已经发展到近三十个，各地的分支都有许多员工通过互联网展开工作。通过在分支出口路由部署深信服上网行为管理，开启 IPSec VPN 模块，与总部的 VPN 设备组建虚拟专用网。实现分支员工身份统一认证、出口带宽流量管控、业务无关行为封堵、上网行为合规记录。总部部署 SC 集中管理平台，进行全网设备的可视化管理，建设一个高效、安全的工作网络，保证员工都能享受流畅、安全的网络体验，愉快的开展工作。

王府井百货

王府井百货各分支商场通过部署深信服上网行为管理，统一对无线网络进行有效管控，同时在总部部署集中管理平台，实现分支用户统一管理、分支设备集中管控以及策略的统一调配。在结合了各项增值推广功能后，王府井的无线网络展现出了无限活力，建设起统一的、高标准的无线网络，在方便顾客无线上网的同时进行针对性营销活动，以及提供额外的售前售后服务，为顾客提供更好购物体验。