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

深信服上网行为管理主打PPT

让上网可视可控，让数据更有价值

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

一．让上网可视可控
二．让数据更有价值

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

让上网可视可控

为什么上网需要可视可控?

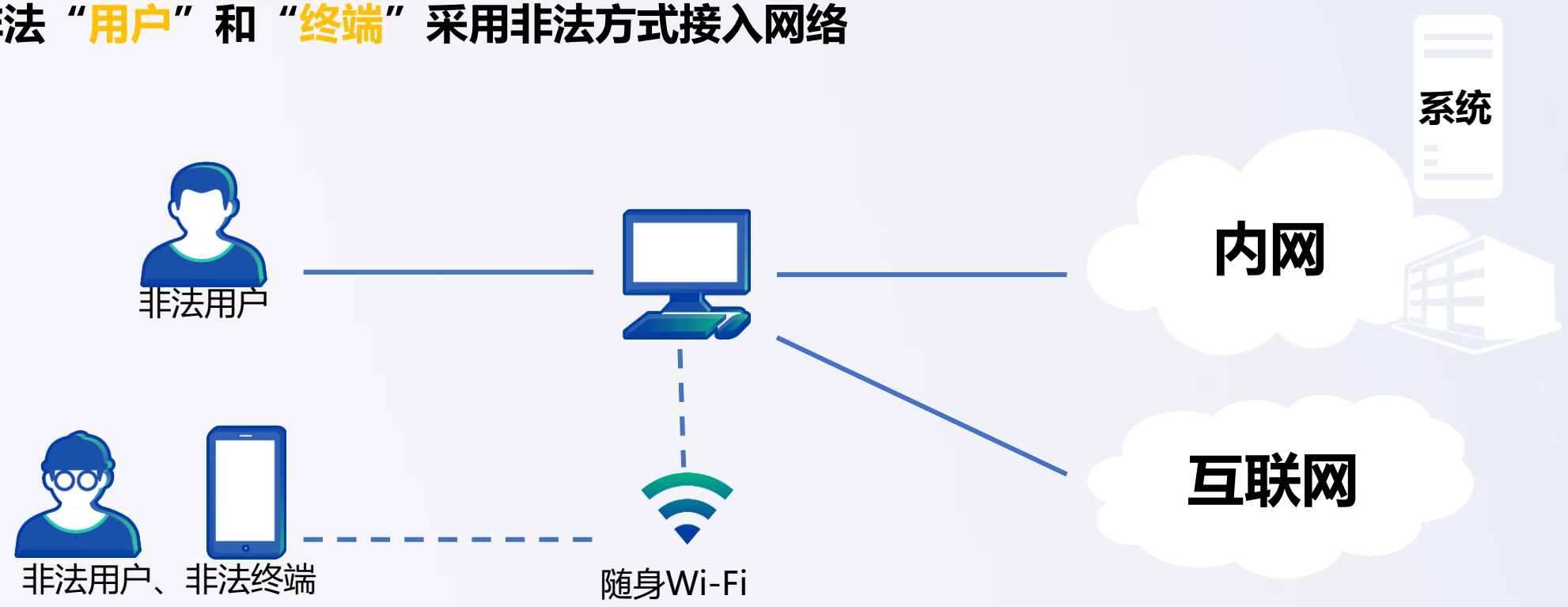
互联网看不见也摸不着，因此往往给内部带来各类威胁

看似正常的上网行为，实际上隐藏着巨大的“看不见管不住”风险

为什么上网需要可视可控?

1、身份风险

非法“用户”和“终端”采用非法方式接入网络

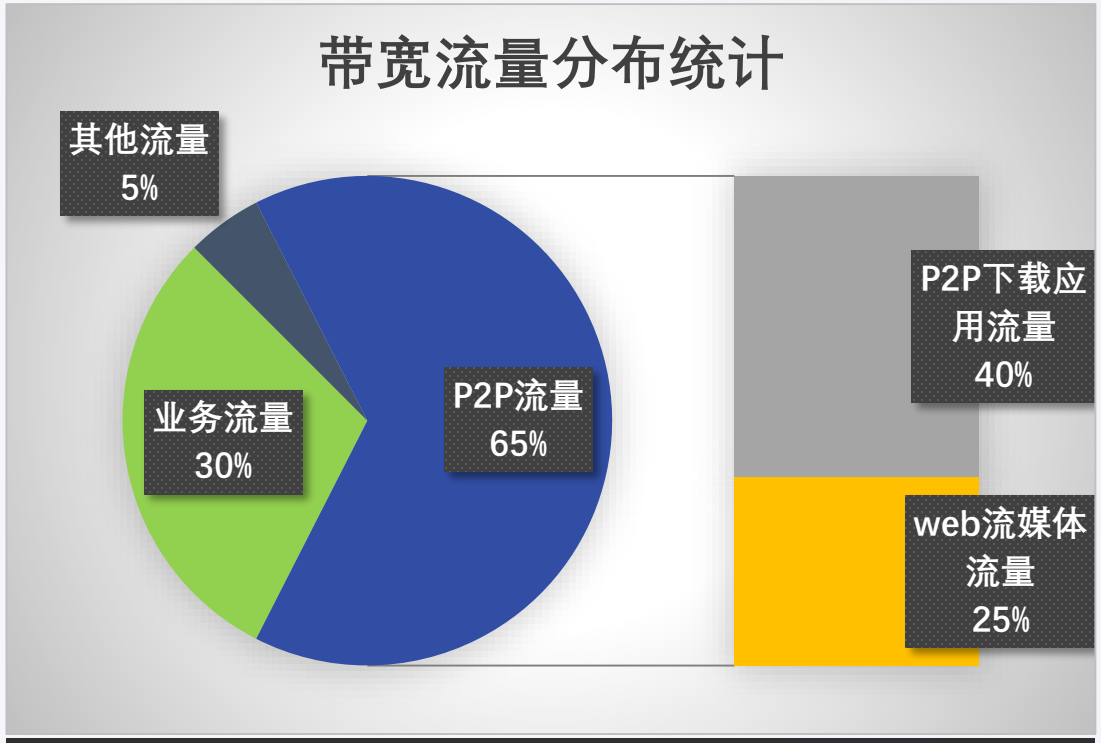


- 外来人员可轻易接入组织内网，窃取内部核心资料，甚至破坏内部网络；
- 随身Wi-Fi等将内网暴露在无线中，更容易被非法用户入侵；
- 不安全终端接入网络，给内网环境带来极大的威胁，如导致病毒内网疯狂传播；

为什么上网需要可视可控?

2、流量风险

识不全、管不住的“P2P流量”，占用大量带宽，影响业务应用正常进行；



P2P流量泛滥，占用大量带宽

50%～90%的互联网带宽被P2P流量抢占；

SAAS业务应用流量无法保障

视频会议、ERP大多为SAAS应用，但访问流量无法保障；

为什么上网需要可视可控?

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

3、行为风险

加密流量巨增，上网行为不可控，数据泄密及网络违法等风险增多；

加密导致风险增大：随着https的大力推广，加密流量占比超过一半，违规风险行为无法及时识别；

网络违法：利用组织网络进行网络造谣、人身攻击，肆意外发反动、赌博、色情信息，遭受法律追究；

外发泄密：敏感数据/文件被随意外发，如个人隐私信息、组织机密信息、政务红头文件等；

如何实现上网可视可控?

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

用户	流量	行为
非法移动终端	流媒体流量	色情网站 工作技术论坛
非法用户	迅雷下载流量	翻墙软件 网盘下载资料
合法终端	发送邮件流量	逛淘宝网 工作OA应用
合法用户	视频会议流量	收发邮件 发布造谣言论
	SAAS应用流量	微信交流 浏览反动论坛

可 视 可 控

用户的可视可控

如何实现“用户”的可视可控?

身份识别 → 更简便：结合现有系统和场景，识别用户身份

接入方式 → 更安全：快速识别接入终端类型，封堵非法接入

终端安全 → 更智能：自主终端安全检查，不合规隔离

上网权限策略

基于不同用户、不同终端以及不同接入方式划分权限策略;

用户的可视可控

1. 多样化认证方式，识别用户真实身份

密码认证

本地密码认证、第三方服务器密码认证

短信认证、微信认证

手机号、微信OPEN ID等信息

单点登录

结合AD域、radius服务器等实现单点登录

Portal认证

支持与多种无线控制器结合，有线无线统一认证；

IP/MAC绑定

绑定IP和MAC信息，支持跨三层取MAC

特色认证方式

二维码认证：接待访客人员，扫一扫上网；

Dkey认证：特殊人员插KEY上网；

多种上网认证和入网认证

用户的可视可控

2. 终端安全检查，不合规终端隔离，禁止入网

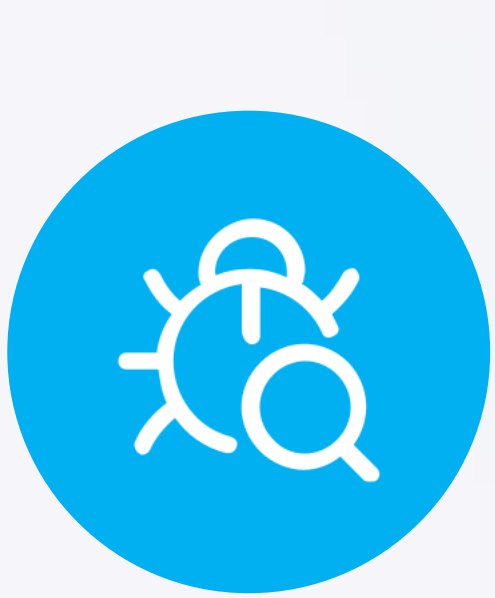
合规检查内容项

- 操作系统检查
- 补丁检查
- 防病毒软件安装检查
- 可疑文件检查
- 注册表检查

不合规终端禁止接入网络，提高内网环境的安全性！

用户的可视可控

3. 及时封堵非法接入的终端



识别终端类型及接入方式

区分PC、移动（IOS、安卓）等终端类型

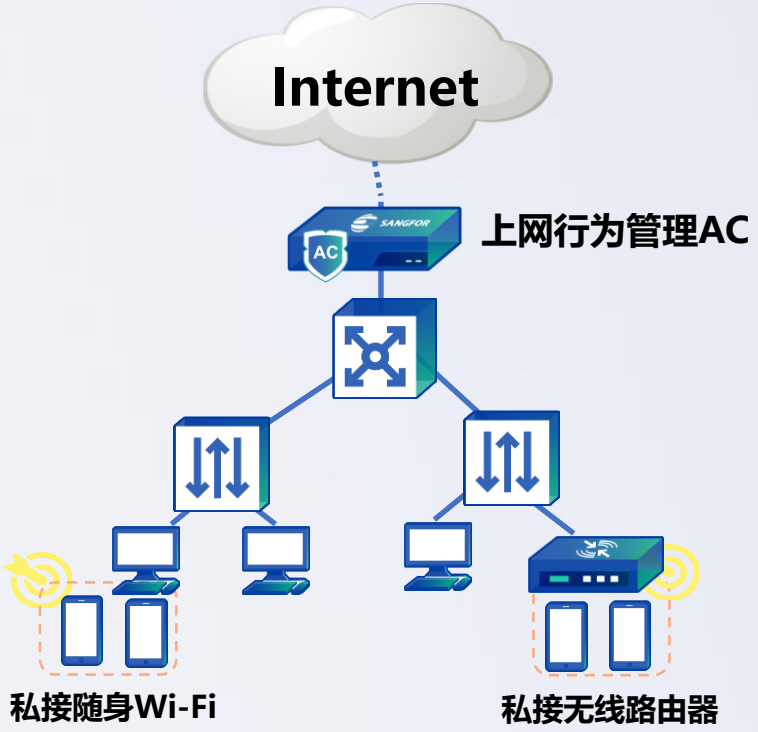
各类型终端的数量

各种上网认证的人数

管控非法接入的无线终端

多种技术手段识别非法接入的终端

立即封堵，并迅速告警



流量的可视可控

如何实现“流量”的可视可控?

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，用户体验最大化
- 从一刀切封堵，到疏堵结合，兼顾业务和体验

更全更准

更人性化

流量识别识别更全、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

流量的可视可控

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

1. 带宽分析 流量的可视化分析

分析带宽的使用情况，给出带宽评级，并直观展现应用的流量分布情况。

2. 多级父子通道 精细化管控

通道化

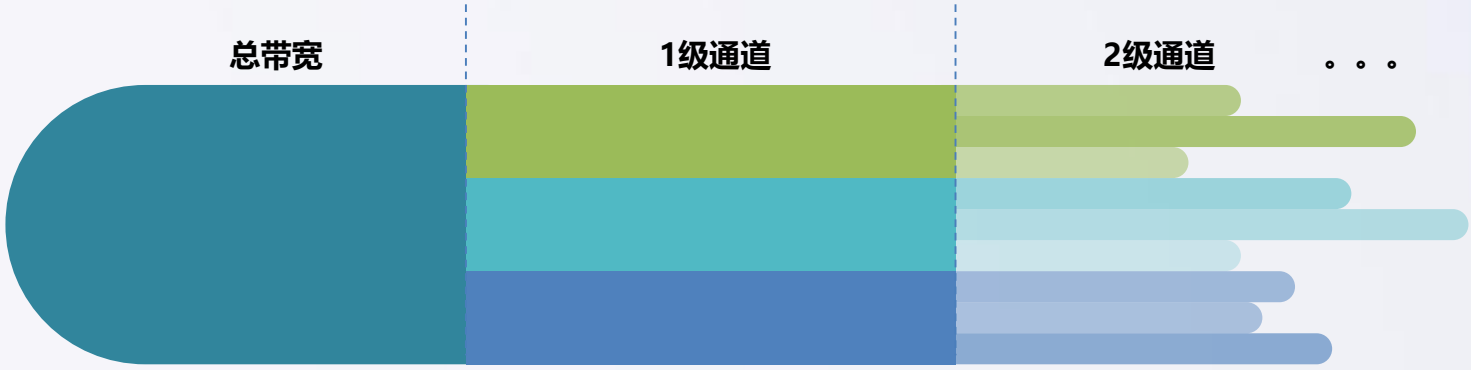
将总体带宽细分通道化，可根据用户或应用进行划分

限制/保证带宽

根据用户或应用的重要性，通道可设置为带宽限制或带宽保证

8级父子通道

最高支持7级通道，匹配组织架构，实现带宽精细划分

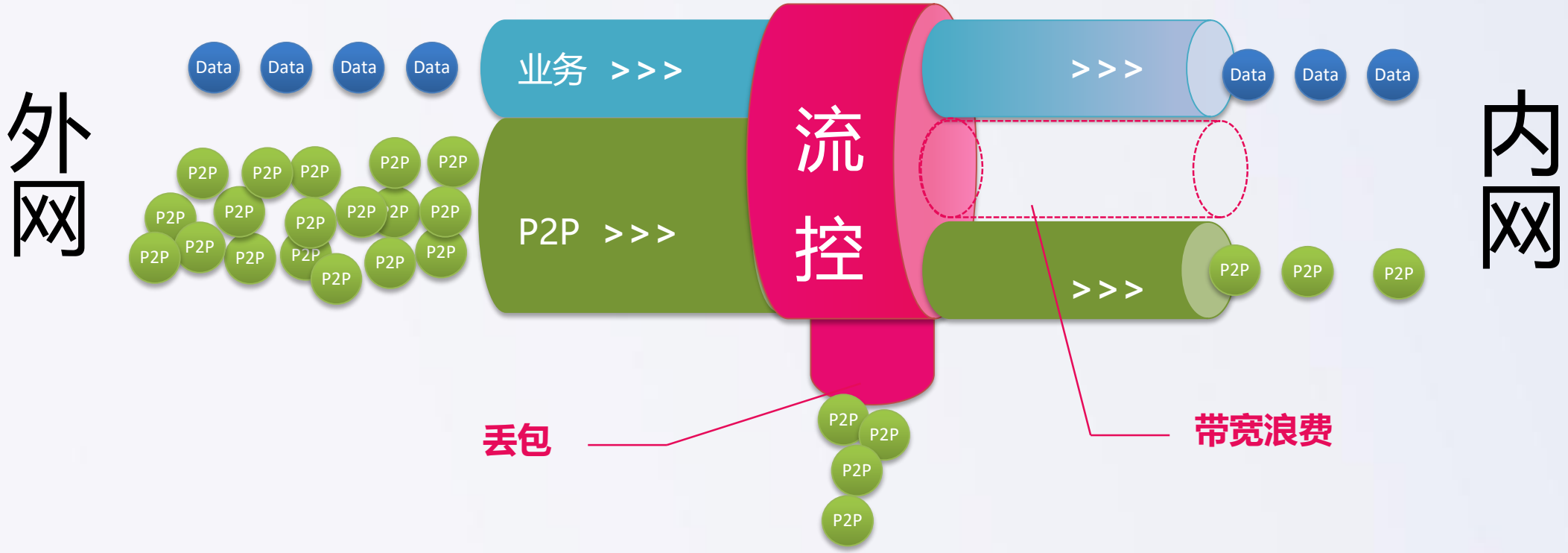


流量的可视可控

3.P2P智能流量管控技术 vs 传统流控

传统流控针对P2P流量已经失效：基于缓存丢包方式，UDP协议自身没有速率调整机制，且

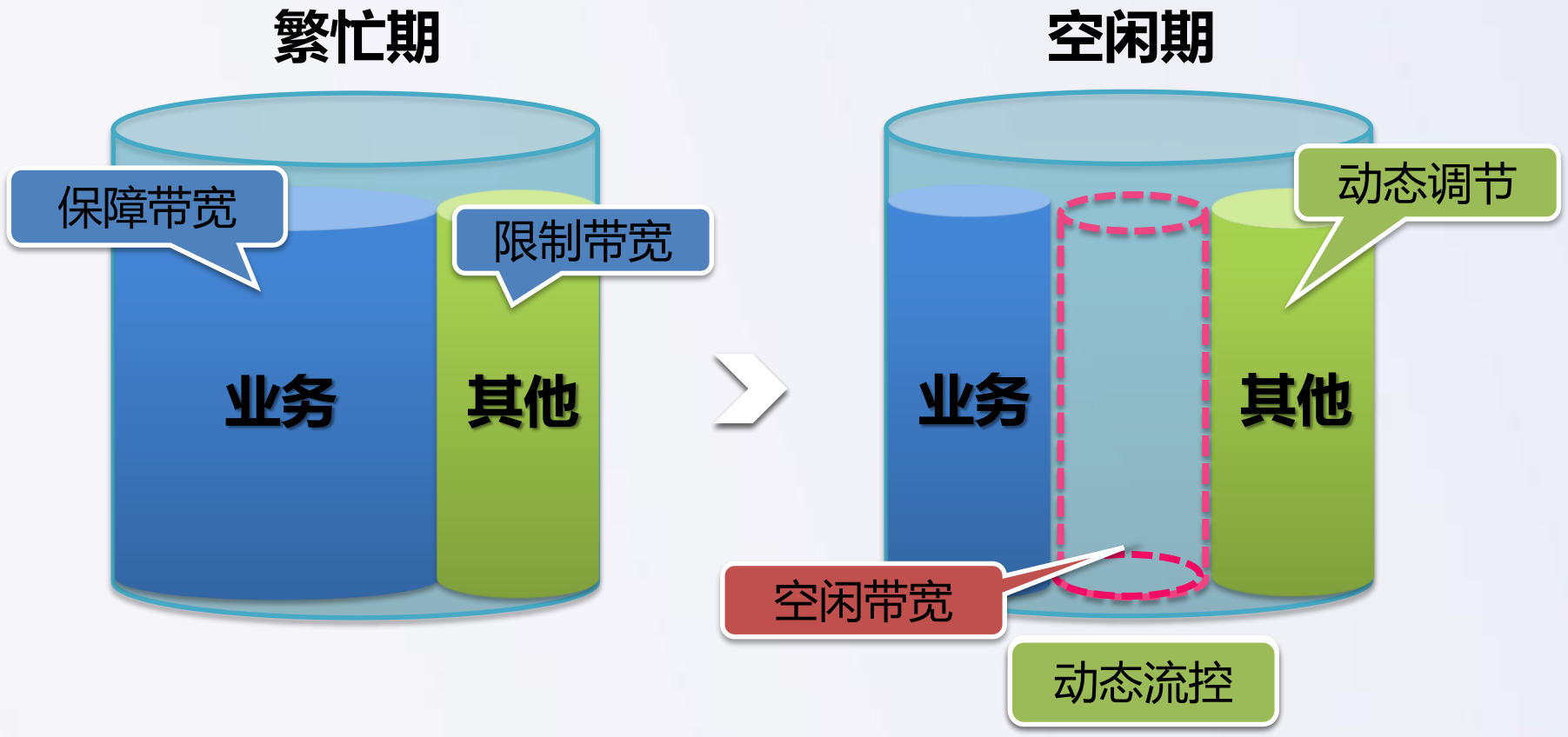
P2P传输模式具有特殊性，外网线路依然被大量的P2P数据报文所占用，导致带宽浪费。



传统流控能够丢弃P2P报文，但是保障不了核心业务！

4. 动态流控　提高带宽利用率

设定阈值(%)来区分空闲和繁忙状态，当整体带宽利用率低于阈值时，通道的最大带宽限制将上浮，直到整体利用率超过了阈值，才回收上浮的部分，实现带宽利用率最大化



流量的可视可控

5. 流控黑名单 疏堵结合 提高用户体验

当某个用户应用的流量、流速、时长超过了限额时：

堵： 将该用户“业务无关的应用”流量划分到流量惩罚通道中进行限速

疏： 将该用户“必要业务应用”流量划分到保障通道，确保业务不受影响

合理分配带宽、更加人性化，提高了用户体验，缓和内部矛盾

行为的可视可控

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

如何实现“行为”的可视可控?

全面准确识别应用

- 完善的URL库
- 全面应用特征识别库
- 持续快速的更新迭代

精细的应用管控

- 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
  - —自定义类别
- 识别应用的细分功能
  - —封堵风险动作
  - —放通实用动作

风险应用和内容监控

- SSL加密内容审计（邮箱、https上传等）
- 翻墙代理软件管控

全面完整的行为记录

- 网页访问审计
- 微博论坛审计
- 邮件审计
- IM聊天内容审计
- 专业的审计KEY

识别和管控应用 → 更细致的管控应用 → 风险应用内容控制 → 全面的行为记录

行为的可视可控

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

1.完善的应用识别技术

全面准确识别常用应用和网站

- **5800+**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2周更新一次，已持续12年
- 老旧应用及时淘汰

2.业务角度管控应用（应用标签化）

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，应用数量众多，容易错配漏配，标签化让应用管理**更准确、简单**

行为的可视可控

3.精细化管控应用的“好功能”和“坏功能”

应用识别需要**能够区分开应用细分动作的好坏**，才能让管控更加**精准和人性化**

区分功能

•微信论坛微博等应用，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

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

4.SSL加密内容识别技术

深信服SSL加密内容识别专利技术

通过深信服独有的针对加密的网页、邮箱等，进行关键字过滤和内容审计

通过配置URL列表，对列表中指定的SSL加密网站或Web邮箱进行过滤和审计。

Baidu 百度　MOil QQ邮箱 mail.qq.com

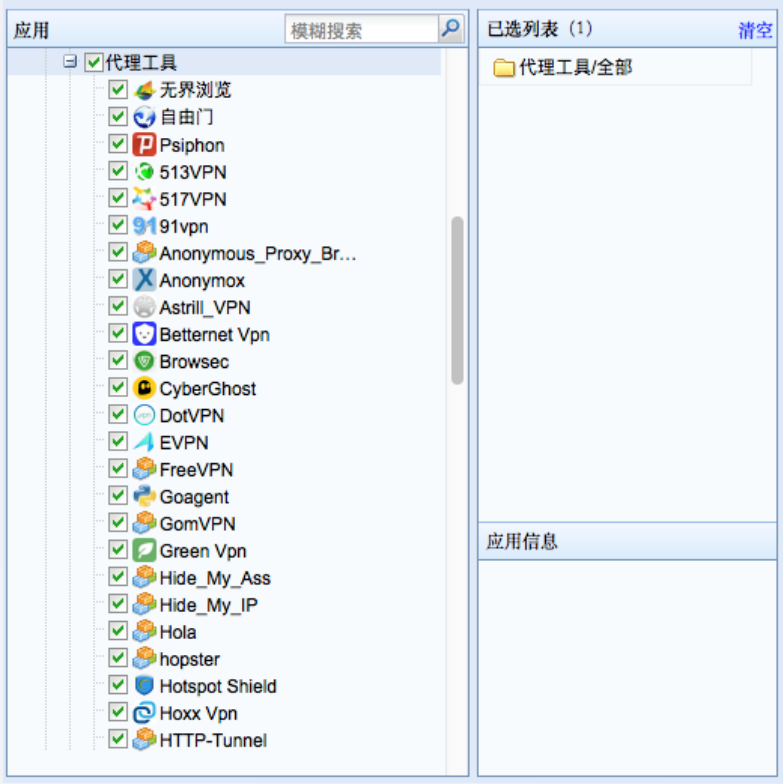
“百度网页”和“QQ邮箱”都已经默认采用SSL加密方式

全面过滤、审计，避免机密内容通过加密网站、邮件外发。

行为的可视可控

5.持续更新的防代理技术和代理应用

- 可禁止使用外部HTTP、Sock4/5代理；
- 可封堵无界、自由门、在线代理等翻墙行为，规避网络违法违规；



防止非法内容通过非法途径绕过网络监管，形成网络安全隐患

行为的可视可控

6.全面的行为记录

Web应用审计

网页访问审计、微博论坛、新闻评论等

IM聊天内容审计

微信和QQ的聊天内容、发文件等

移动APP审计

账号审计、内容审计（非加密类应用）、应用行为审计

免审计KEY(紫)

用户使用免审计USB-KEY后，其上网行为将不会留下日志记录，避免机密信息外泄。适用于特殊人员。

日志审计KEY(棕)

管理员只能通过使用日志审计USB-KEY才能获得日志查看权限，保护敏感数据。

保护敏感日志，专门的审计KEY

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

让数据更有价值

让数据更有价值

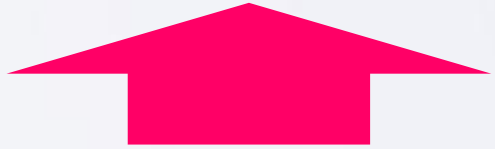
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

如何实现数据价值?

基于海量的上网行为数据，对用户行为特征进行深度建模分析，及时分析内部风险行为，持续挖掘数据价值。

深信服为客户提供完善的查询追溯和丰富的数据分析报表

完善的事后查询追溯+丰富的数据分析报表



外置数据中心

网站、IM、邮件、发帖等所有上网行为查询

应用、流量、时长等数据统计

数据真实还原

多维度统计

数据下钻查询

“百度式”搜索中心

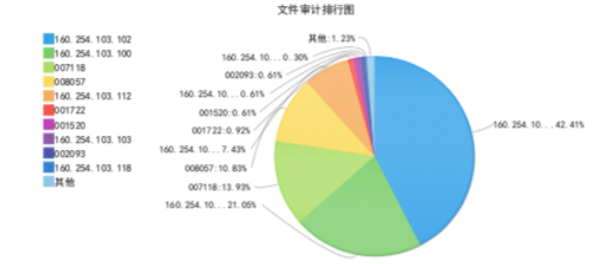
各类上网行为：用户账号、手机号、微信ID、各种虚拟账号、用户浏览的网站、搜索的关键字、发送的邮件、论坛发帖、发布的微博、IM聊天内容等

让数据更有价值

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

丰富的数据分析报表

1.1、用户行为分析 - 文件审计排行



文件审计排行

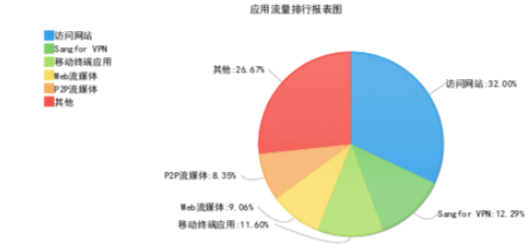
	用户名	组名	源IP	发送方式	文件类型	发送次数	次数占比
1	160.254.103.102	/特殊员工组	160.254.103.102	1	图片:105 未知类型:29 压缩文件:3	137	42.41%
2	160.254.103.100	/特殊员工组	160.254.103.100	1	未知类型:54 压缩文件:14	68	21.05%
3	007118	/经理室	160.254.103.35	1	未知类型:45	45	13.93%
4	008057	/经理室	160.254.103.36	1	未知类型:34 压缩文件:1	35	10.83%
5	160.254.103.112	/特殊员工组	160.254.103.112	1	未知类型:24	24	7.43%
6	001722	/员工组	160.254.103.33	1	未知类型:2 压缩文件:1	3	0.92%
7	001520	/员工组	160.254.103.49	1	未知类型:2	2	0.61%
8	160.254.103.103	/特殊员工组	160.254.103.103	1	未知类型:2	2	0.61%
9	002093	/员工组	160.254.103.37	1	未知类型:2	2	0.61%
10	160.254.103.118	/客户组	160.254.103.118	1	未知类型:1	1	0.30%
11	其他	-	-	-	-	4	1.23%
12	所有用户	-	-	-	-	323	100.00%

1.1、网站分类分析 - 网站分类行为趋势

网站分类行为趋势

	用户名	记录	拒绝	行为总次数	占比
1	160.254.103.102	2138	0	2138	15.15%
2	160.254.103.100	1789	0	1789	12.67%
3	160.254.103.118	1147	0	1147	8.12%
4	160.254.103.112	1024	0	1024	7.25%
5	001520	875	0	875	6.20%
6	所有用户	14110	0	14110	100.00%

1.2、流量报表 - 应用流量排行报表



应用流量排行报表

	应用类型	用户名	具体应用	上行流量	下行流量	总流量	总流量占比
1	访问网站	160.254.103.100:104.31Gb 160.254.103.102:37.68Gb 160.254.103.118:11.83Gb 其他:82.7Gb	IT框架:44.1Gb 在线影音及下载:17.36Gb 华泰白名单3_区域_华泰联合:15.14Gb 其他:159.92Gb	24.01Gb	212.5Gb	236.51Gb	32.00%
2	Sangfor VPN	sangfor_vpn:90.83Gb 其他:10.01Mb	Sangfor VPN:90.84Gb	11.83Gb	79.01Gb	90.84Gb	12.29%
3	移动终端应用	160.254.103.102:34.55Gb 160.254.103.118:19.79Gb 160.254.103.100:19.26Gb 其他:12.19Gb	App Store:45.93Gb 微信:12.06Gb 淘宝天猫:5.14Gb 其他:22.67Gb	3.9Gb	81.9Gb	85.8Gb	11.60%
4	Web流媒体	160.254.103.100:55.04Gb 160.254.103.102:3.44Gb 160.254.103.226:2.82Gb 其他:5.7Gb	腾讯视频:51.5Gb MP4视频:11.43Gb 中国网络电视台视频:2.44Gb 其他:1.63Gb	1.25Gb	65.75Gb	66.99Gb	9.06%
5	P2P流媒体	160.254.103.101:56.39Gb 160.254.103.102:4.97Gb 160.254.103.100:190.21Mb 其他:200.13Mb	PPTV:56.25Gb PPStream:2.6Gb 暴风影音:2.18Gb 其他:725.24Mb	44.76Gb	16.99Gb	61.75Gb	8.35%
6	其他	-	-	32.15Gb	164.98Gb	197.13Gb	26.67%

让数据更有价值

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

在此基础上，深信服创新提出——行为感知系统

网页访问记录

移动应用记录

发邮件、发帖、
发微博等外发记录

其他上网记录等

AC数据

行为感知系统

底层技术

MapReduce框架
列式存储

建模分析

机器学习
图计算等

场景应用

应用商店
行为感知应用

APP式分析呈现

让数据更有价值

场景式行为感知应用

行为风险可视场景

政府企业场景：


泄密风险追踪


离职倾向分析


工作效率分析

教育学校场景：


校园网贷分析


学生沉迷网络


图书馆资源优化

简化网络运维管理场景

广域网多分支场景：


全网上网态势分析


分支网络监测运维


专线质量分析

办公网场景：


办公网上网态势分析


带宽分析


未关机检测分析

让数据更有价值

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

泄密追踪分析

风险场景

- 单位内部有大量核心资料和敏信息，一旦外泄，造成严重损失
- 内部泄密后，缺乏追踪手段

应用介绍

- 外发概括：整体掌握外发风险，分析外发次数、类型、通路等情况
- 泄密追溯：上传文件和关键词，追溯存在外发风险的人
- 风险预警：设置敏感信息和文件，一旦发现外发，迅速告警

让数据更有价值

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

校园网贷分析

风险场景

- 多起校园网贷事件影响恶劣
- 教育部多次发文防范校园网贷风险
- 深圳、广州、重庆等地出台规范校园网贷

应用介绍

- 分析网贷行为，给出高危发生网贷和关注网贷的学生名单，以及判断依据
- 帮助学校及时发现网贷学生，尽早进行引导教育

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

THANK YOU