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

深信服全网行为管理AC主打PPT

全网行为可视可控，内部风险智能感知

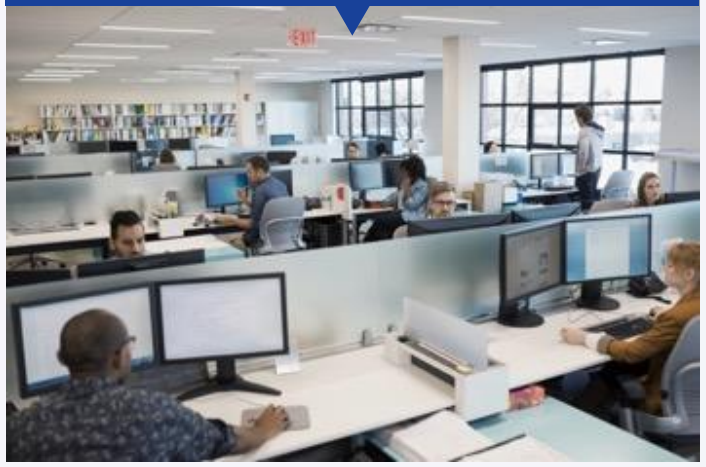
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

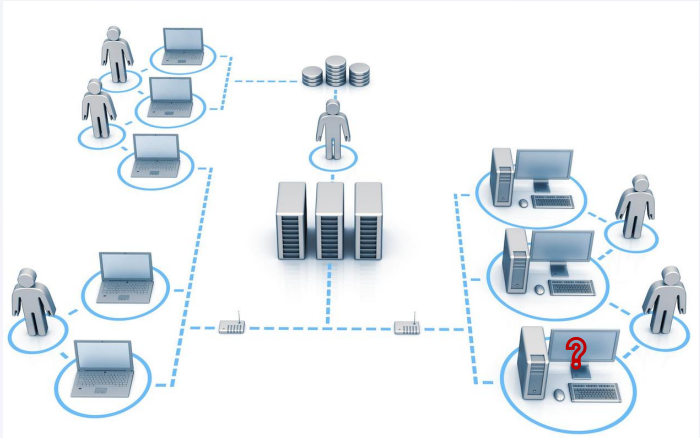
内部行为风险大，难管控

企业内部面临各种行为风险挑战

挑战1

员工上网行为随意，上网体验差，容易影响办公效率，带来违法违规风险



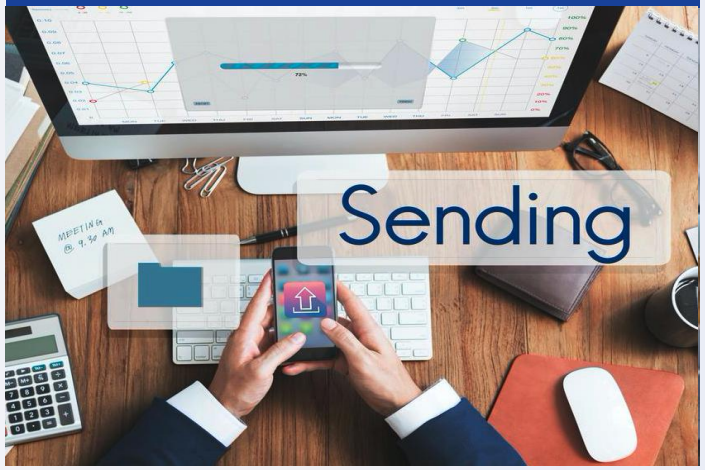


挑战2

非法用户和终端入网，容易将不安全因素带入内网，导致终端感染病毒和数据窃取风险剧增

挑战3

数据经常通过外设、网络应用传输和共享，容易造成敏感数据泄密，且难发现、难追溯



挑战1：

员工上网行为随意，上网体验差，容易影响办公效率，带来违法违规风险

工作效率低

办公室沦为免费网吧，员工上班时间进行娱乐应用（如游戏、购物等）占用大量时间，影响工作效率；

上网体验差

无关应用占用大量带宽，云端业务、SAAS应用（视频会议、邮箱等），访问体验无法保障；

网络违法

利用办公网络肆意外发反动、造谣、赌博、色情等信息，给公司和组织造成极大损害，且遭受法律追究；

挑战2:

非法用户和终端入网，容易将不安全因素带入内网，导致终端病毒感染和数据窃取风险剧增

终端非法接入

外来人员随意可接入内网（访客/合作伙伴/下游等），插上网线即可接入到内部网络，容易攻击内网业务和窃取内部数据。

内网终端非法外联

内部员工私自将内网中禁止连接互联网的终端通过各种方式接入互联网；终端可能会被感染病毒，再接入内网会存在重大的安全隐患及泄密风险

不合规终端入网

因未安装杀毒软件、不合规操作系统、终端使用弱密码等不合规终端接入网络，给内网环境带来极大的威胁，比如导致病毒内网疯狂传播（勒索病毒）

网络终端不可视、难管理

移动终端和IOT设备不断增多，不清楚内网有哪些终端设备，无法实现管控，管控存在视野盲区；

挑战3:

数据经常通过外设、网络应用传输和共享，容易造成敏感数据泄密，且难发现、难追溯

网络数据外发

IM工具外发
网盘/云笔记外发
邮件外发
论坛/贴吧上传
FTP上传
其他SAAS应用外发
网络共享（私接服务器）

终端数据外发

移动存储拷贝
打印机打印外带
多网卡外发
远程桌面共享
离网终端外发

敏感数据不可视

敏感数据外发泄漏
核心数据违规滥用
数据泄漏难定位

内部行为安全的相关法律要求

组织网络安全建设不满足国家法令法规要求，一旦出现网络数据泄漏、留存审计不合规、内网非法入网等将面临行政处罚。

网络安全法

第三章　网络运行安全

第一节 一般规定

第二十一条　国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

网络安全等级保护2.0

7.1.2.3　安全审计（G3）

本项要求包括：

a）应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；

b）审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c）应能够根据记录数据进行分析，并生成审计报表；

d）应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

网络架构	**a）应保证网络设备的业务处理能力满足业务高峰期需要；**
	b）应保证网络各个部分的带宽满足业务高峰期需要；
边界防护	**b）应能够对非授权设备私自联到内部网络的行为进行检查或限制；**
	c）应能够对内部用户非授权联到外部网络的行为进行检查或限制；

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

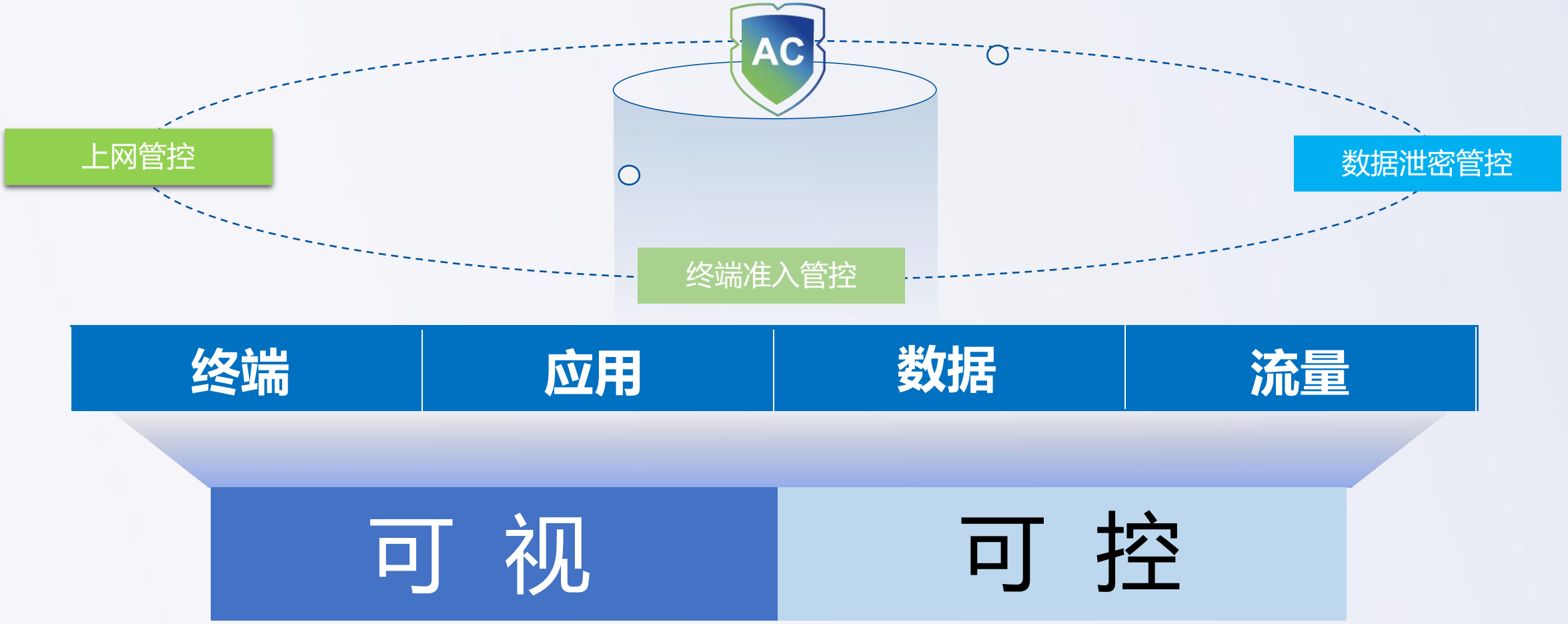
以人为核心，实现安全管控一体化

建设以人为核心的安全管控体系

—你是谁	—你能做什么	—你做了什么	—有哪些风险
认准内部用户终端	**管好用户全网行为**	**记录全局行为内容**	**看清内部行为风险**
▪ 对网络接入进行有效控制是保证网络安全的前提 ▪ 完善有效的网络准入机制	▪ 基于组织架构的权限控制是保障内部安全的基础 ▪ 网络应用访问权限 ▪ 数据外发行为权限	▪ 全面的行为监测及审计是发现和追溯内部风险的重要手段 ▪ 互联网应用、业务应用、终端行为的行为记录	▪ 通过全网行为数据关联分析，实现全网风险可视 ▪ 用户行为画像和行为风险可视

深信服全网行为管理产品理念

内部风险智能感知，全网行为可视可控：通过全网终端、应用、数据和流量的可视可控，智能感知终端违规接入、敏感数据泄密、上网违规行为等内部风险，解决上网管控、终端准入管控和数据泄密管控的一体化管控。



核心价值一

保障上网规范和上网体验，避免违法违规，减少上网抱怨

精细的识别管控

●完善的URL库和应用特征识别库，持续更新

●应用分类标签管控
—降低工作效率类
—SAAS业务类

●应用细分管控
—封堵风险动作
—放通实用动作

灵活的流量管控

●精细化管控与保障
—多级父子通道管控
—SAAS业务流量保障
—流控黑名单机制

●流量智能调控
- 动态流控
- 多线路灵活调度
- 智能应用选路

更上网安全管控

- 风险应用管控
  —翻墙代理工具
  —远程桌面工具
- 终端上网安全
  —SAVE文件杀毒
  —恶意链接检测过滤
  —僵尸主机检测管控

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

更细致的应用管控 → 更灵活的流量管控 → 更安全的上网管控 → 全面的行为记录

核心价值二

建立终端入网安全规范，降低安全隐患和数据泄露风险

核心价值三

建立数据外发规范，分析风险，防止敏感数据泄露

网

网络数据外发管控
网络外发管控与审计
SAAS应用外发管控与审计

端

终端数据外发管控
U盘拷贝管控与审计
离网终端管控与审计

业务

业务数据访问监控
业务应用访问操作监控
SAAS业务应用访问操作监控

数据泄密分析

- 泄密风险预警
- 敏感内容识别
- 数据外发可视
- 数据违规滥用
- 泄密事件追溯

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

全网行为管理核心优势

核心优势1:安全管控一体化

行为安全管控从碎片化到一体化

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

管控碎片化

单个类别的安全管控产品

- 部署多套管控设备，运维复杂、成本高、无法实现联动
  - 上网行为管理设备
  - 终端准入设备
  - 数据DLP设备
- 各种终端Agent影响性能，抱怨不断

各种终端Agnet

安全管控一体化

构建安全管控一体化

- 全网统一管控
- 管控简单易用

行为安全管控一体化的落地方案

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

- **全网统一管控**

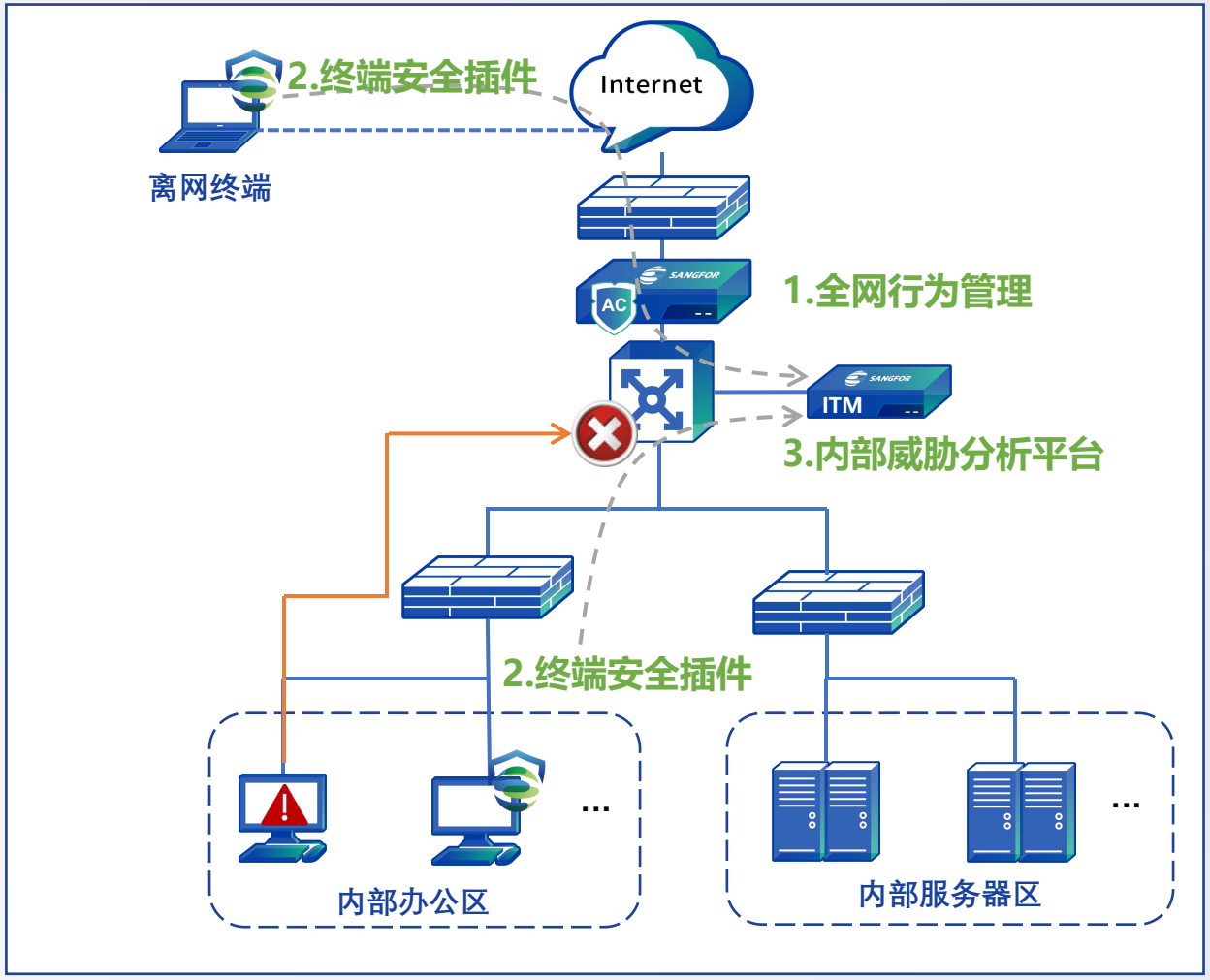
  一个产品解决上网行为管理、终端准入、数据泄密管控问题，实现全局统一管控，降低建设成本、简化运维。

- **终端管控插件融合**

  一个客户端解决终端准入、终端管控、杀毒，按需使用平滑扩容，减轻终端性能压力，让管理易落地。

- **行为风险综合分析**

  基于全网行为数据采集，构建人、资产、行为的完整风险分析画像；基于先进的UEBA模型等技术，及时发现数据泄密、上网违规、非法接入等内部风险。



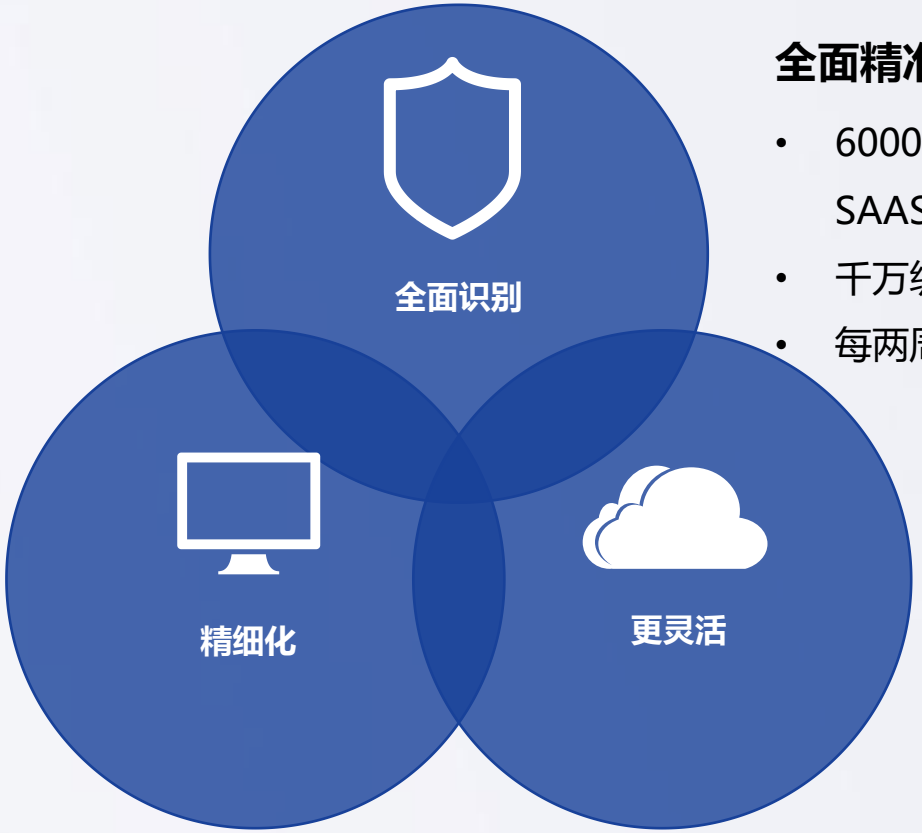
核心优势2:上网可视可控

应用精细化管控

全面识别并精细管控上网应用，保障落地上网规范要求

应用细分管控，减少风险

- 区分细分功能管控，如可浏览论坛，但禁止发帖，降低违法风险；
- 区分方向管控，如远程桌面，区分发起远程和接受远程等方向，防止电脑被远程控制



全面精准识别常用应用和网站

- 6000+种应用、1000+移动应用、100种SAAS应用
- 千万级URL分类库
- 每两周更新一次，持续12年

更灵活的上网权限策略

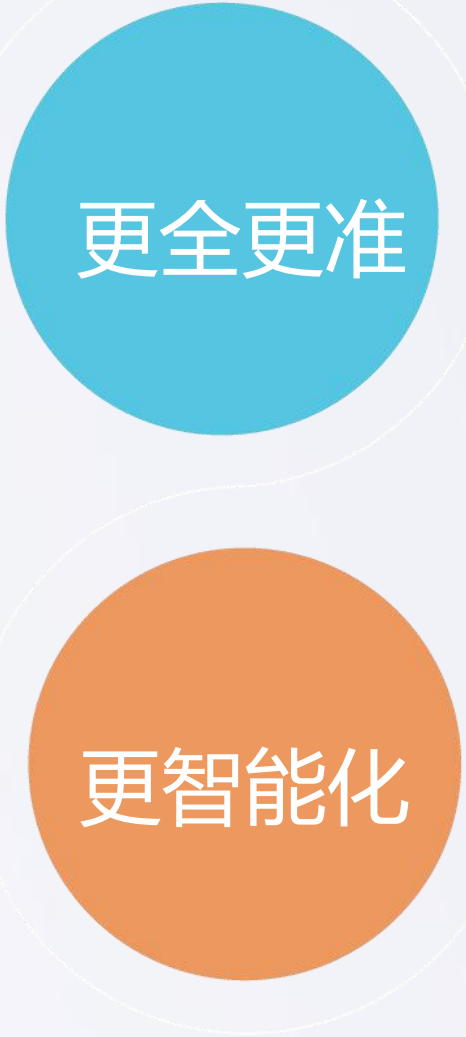
- 依据用户身份、时间空间、终端类型灵活分配上网权限，满足各种场景的管理诉求
- 从业务角度对应用进行标签化分类，管控更高效、更简单

流量智能优化

灵活智能的带宽管控和流量优化，保障上网体验，减少员工抱怨

更智能的流量优化策略

- 从单级策略到多级父子通道，匹配组织架构更加灵活
- 从静态策略，到动态流控，用户体验最大化
- 重要应用智能分配最优线路，保障业务应用以及SAAS业务使用体验



流量识别更全、更准

- 应用流量识别全面
  - 全流量识别P2P流量，准确控制P2P下行流量
  - 全面识别视频会议、远程办公等SAAS业务应用流量
- 多种维度流量统计
  - 基于用户、终端类型、文件类型、时间等

全面的行为内容审计

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

全面记录上网行为内容，完善的查询追溯，满足内部监控和外部合规要求

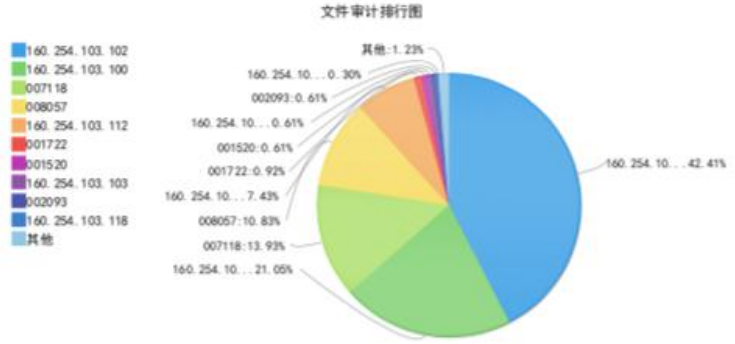
3类行为

- 全面详细的行为内容审计，审计元素非常全面，方便事后追溯查询。
- 先进完善的https网页全解密和加密应用内容审计，保障审计无遗漏。

4大核心元素审计

- **身份账号** – 账号、虚拟身份
- **应用流量** – 应用名称类别，流量时长大小
- **行为动作**–浏览、上传、下载、发送、拷贝等
- **内容数据** –留言、聊天信息、文件等

1.1、用户行为分析 - 文件审计排行



文件审计排行

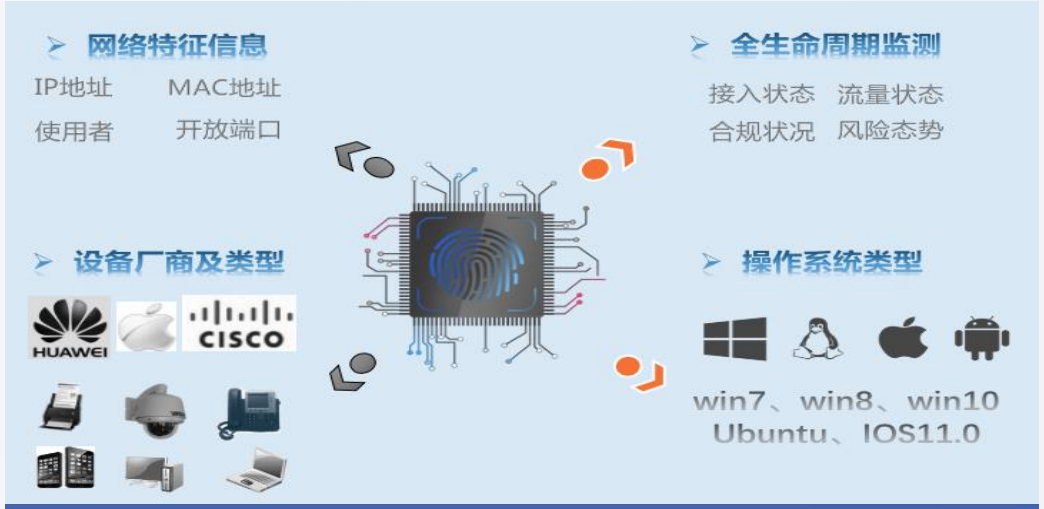
	用户名	组名	源IP	发送方式	文件类型	发送次数	次数占比
1	160.254.103.102	/特殊员工组	160.254.103.102	1	图片:105 未知类型:29 压缩文件:3	137	42.41%
2	160.254.103.100	/特殊员工组	160.254.103.100	1	未知类型:54 压缩文件:14	68	21.05%
3	007118	/经理室	160.254.103.35	1	未知类型:45	45	13.93%
4	008057	/经理室	160.254.103.36	1	未知类型:34 压缩文件:1	35	10.83%
5	160.254.103.112	/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%

核心优势2:终端准入可视可控

全网终端入网状态可视

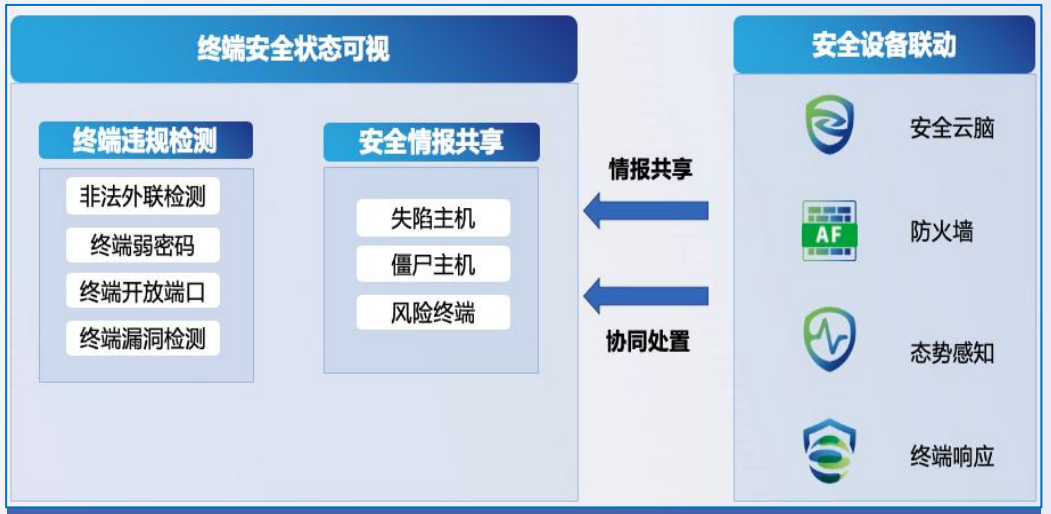
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

掌控全网终端的接入状态和安全状态，掌控全网有哪些终端，终端是否安全



自动识别入网终端及其详细指纹信息，实现终端从接入状态到行为流量全流程的监测，方便运维管理

终端入网状态全掌握



持续监测终端违规行为，和安全产品联动，实现终端风险全面感知，及时处置风险终端

终端安全状态全感知

全网终端接入状态可视

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

终端接入状态、网络IP使用情况、终端安全状况可视

全网全终端的接入认证

丰富的认证方式，匹配不同网络环境和终端，满足各种的认证需求

边界入网认证

支持802.1x、MAB认证、旁路无感知认证

Portal认证

支持与多种无线控制器、交换机结合，实现有线无线统一认证

哑终端认证

自动提取终端指纹

从终端指纹、流量特征实现哑终端认证审批

强大的密码认证

本地密码认证、第三方服务器认证、短信认证、OA结合认证等

单点登录

结合AD域、radius服务器等实现单点登录，简化认证体验

特色认证方式

二维码认证：接待访客人员，扫一扫上网；

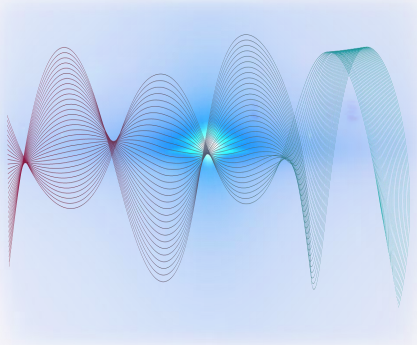
Dkey认证：特殊人员插KEY上网；

自注册：用户完善信息后才可入网

轻量级全终端安全检测

终端安全检查：无端和轻量级端两种方案，全面确保入网终端满足单位安全要求，对违规终端隔离修复。

合规检查



无端流量检测
（无客户端，适用范围广）

- ✓ 杀毒软件安装检测
- ✓ 非法外联违规检测及告警
- ✓ 僵尸主机及恶意URL检测，发现中毒终端
- ✓ NTA异常流量行为分析持续检测安全能力

轻量化插件检测

- ✓ 杀软安装
- ✓ 操作系统版本
- ✓ 注册表键值
- ✓ 补丁情况
- ✓ 非法外联检测
- ✓ 接口开放情况
- ✓ 终端程序运行情况
- ✓ 自定义检测项

终端外设和非法外联精细管控

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

非法外联|外设管控：全面严格控制终端外联行为带来的风险

外设管控

外设管控

支持存储设备（如U盘，手机，平板）、网络设备（如移动数据网卡、无线WIFI网卡、蓝牙适配器共享网络、手机共享网络）、蓝牙设备（如笔记本自带蓝牙、蓝牙适配器等相关功能）、摄像头 、打印机 、及其他可处理的场景

精细化管控

支持移动存储类设备拒绝、只读、可读写、告警、白名单控制

外联监控

外联探测

支持拨号、双网卡、无线、非法WIFI、4G网卡、非法网关、连接外网以及自定义外联等多维度检测能力；发现外联行为马上断网并通知管理员

外联控制

提前梳理好内网安全域网段，利用windows底层技术生成规则，实现外联强管控

核心优势3：数据泄密可视可控

全通路的外发管控与审计

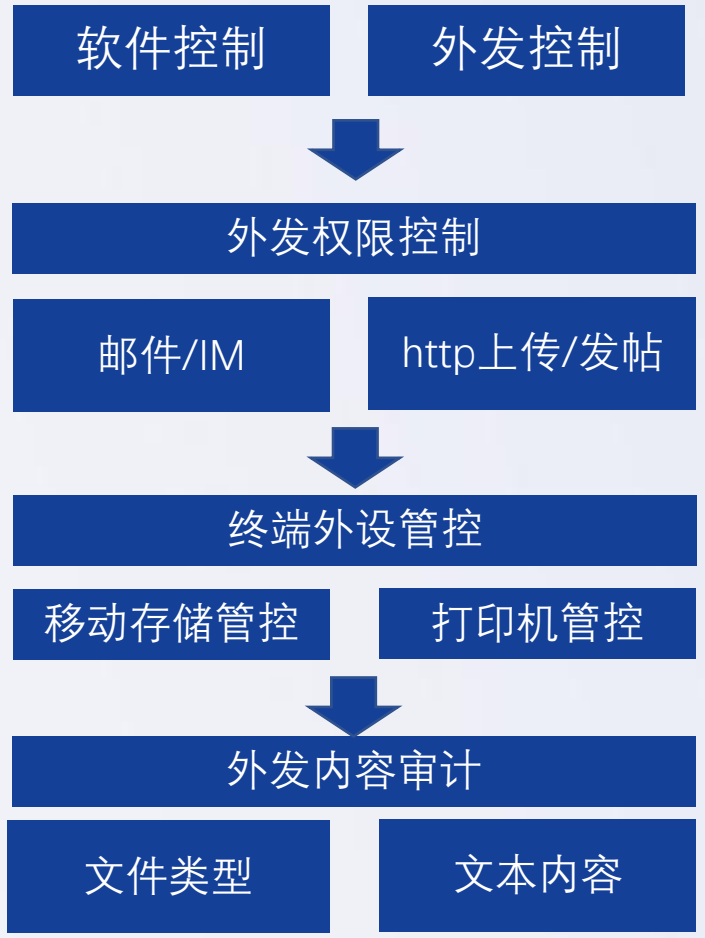
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

全面识别和管控数据外发通路，实现外发数据可视可控，建立数据外发规范，防止敏感信息泄露。

通路全识别

外设通路	U盘，打印机，移动存储，蓝牙，无线网卡
SaaS通路	邮件、IM、网盘、OA协同办公
客户端软件	钉钉、企业微信、微信、QQ、网易邮箱、Exchange、百度网盘
运维通路	RDP、Teamviewer、Xshell、Pshell..
Https通路	网页上传、留言、搜索内容等等

通路可管控可审计



数据泄密风险智能感知

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

泄密规则分析

内置常见泄密规则，支持自定义，精准识别违规行为

数据外发情况可视

对敏感数据和关键通路的外发情况一目了然

异常行为预警

通过UEBA技术发现异常行为，提前进行风险预警

搜索引擎式泄密查询

根据各种泄密源特征和相似度，快速定位外发轨迹和人员。

根据源关键词、文档内容、图片内容，进行全网流动数据的相似度匹配，快速定位外发轨迹和人员。

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

全网行为管理市场品牌

全网AC品牌优势

No.1

- 2006年首先推出行为管理产品
- 中国市场多年销售额排行第一
- 安全审计产品国标主要起草单位
- 2020年首先推出全网行为管理

Gartner

- 连续九年国内唯一入围Gartner SWG魔力象限
- 率先通过国家信息安全产品EAL3高等级认证及IPv6 Ready认证
- 25项专利和30多项媒体奖项

5W

- 累计服务超过5万家客
- 服务80%的世界500强中国企业
- 部委级单位和五大行客户选用

典型客户案例

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

行业	客户名称	行业	客户名称	行业	客户名称	行业	客户名称
政府	深圳市生态环境局	企业	印力集团	政府	上海市松江区人社局	企业	南孚电池
政府	东莞市电子政务办公室	交通	重庆高速公路集团有限公司	司法	海南第二中级人民法院	公安	浙江省公安厅技侦总队
政府	湖南怀化市政府信息中心	交通	广州交通投资集团有限公司	企业	江中集团	交通	重庆高速公路管理
税务	湖北省神农架税务局	金融	金融安徽徽商银行	企业	比亚迪	教育	平谷中学
医院	湖南省常德市妇幼保健院	金融	中国光大银行成都分行	医疗	中山大学附属医院	通信	陕西联通
医院	湖南辰溪县人民医院	金融	中国人民银行成都分行	通信	上海盈联电信	企业	德邦物流
医疗	北京西城区卫计委	教育	湖南岳阳教育局	企业	融创万达	医疗	上海曙光医院

【企业】康佳集团-半导体事业部

康佳集团成立于1980年，是中国改革开放后诞生的第一家中外合资电子企业，已完成多媒体彩电、移动通信、白色家电等业务的公司化运营，同时新成立了科技产业园事业本部、半导体事业部、环保科技事业部等战略新部门，同时投资并购了多家高科技企业，是一家典型高新电子制造业。

2019年，康佳集团新设立的半导体业务线，在重庆开设新厂，由于新业务涉及到专利技术、研发代码、制造工艺、生产数据、财务数据等敏感数据资产，对新业务的研发区域、办公区域、生产制造区域提出数据防泄密、边界隔离、防病毒、容灾高可用等需求。

■ 需求与挑战

康佳新建半导体业务线，要求做信息化建设，由于新业务涉及到专利技术等核心信息资产，针对新业务的研发区域、办公区域、生产制造区域提出了数据防泄密的需求。

一期建设中，客户要求所有内网外发信息（包括HTTPS上传文件、IM聊天外发内容、U盘拷贝文件）等可全面审计，并可通过关键字等方式检索和监管外发信息，从而实现泄密事件可及时预警和溯源追责，研发环境数据不落地。

■ 解决方案

新半导体业务线整体规划为三个板块，研发环境、办公环境、生产制造环境，三个区域物理隔离，结合AC+DLA+桌面云+EDR四款产品为康佳集团交出了满意的答卷：。

1、办公环境：

（1）针对半导体业务办公部门，办公人员包含财务、人事、专利申请等涉及核心数据的重要职能部门，通过桌面云、全网行为管理构建一套安全办公桌面环境。

（2）在网络侧，通过内网出口AC审计外发信息并部署DLA泄密分析平台，通过内置的各类场景建模及智能行为分析，进行泄密检测和预警。

2、研发环境：

通过桌面云终端观看软件实现终端准入、外设管控、桌面水印防拍照、研发文档透明加密；通过部署端点安全组件EDR，有效防范终端失陷；代码管理服务、RTX等业务系统部署在超融合平台，保障应用高可用和数据双备份。

■ 方案价值

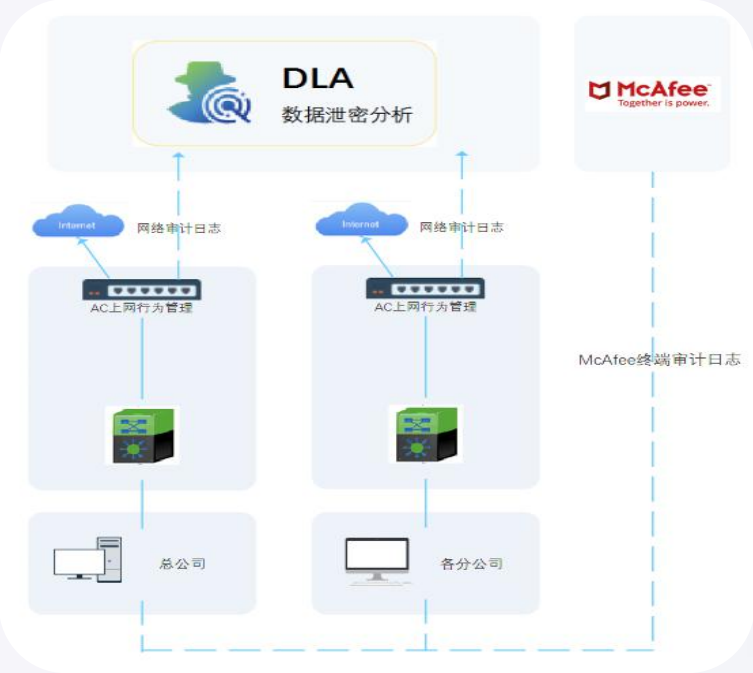
（1）完善防御：从网络攻击防护、终端管控、安全审计、泄密分析、高可用保障等维度，完善防御数据泄密链条。

（2）外发审计：帮助安全管理人员掌握所有外发数据的概括。

（3）泄密分析：从行为及场景分析角度提高泄密分析准确性，实现AI泄密分析。

（4）泄密追溯：根据关键字、段落或文件追溯到泄密员工，发生泄密事件可追责。

【企业】万科集团



万科集团，成立于1984年，经过三十余年的发展，已成为国内领先的城乡建设与生活服务商，公司业务聚焦全国经济最具活力的三大经济圈及中西部重点城市。

■ 需求与挑战

万科集团在全国总人数超过6万人，同时在全国各地拥有多家分支机构，人员众多导致对于各类机密资料的保护困难程度大幅上升，信息部门管理员难以发现泄密行为。

- 万科集团部署了McAfee的终端防泄密，但由于终端误判太多，导致的误判阻断已影响了正常办公，所以，终端防泄密层面，已经退回至告警阶段，不做阻断。
- 2017年，第三方独立审计发现，万科集团存在因QQ/微信、用户上网出口的邮件外发、网盘上传等途径数据传输的追踪分析缺失，可能会增加数据泄密的风险。
- 2018年，发生了严重的泄密事件，但无法从终端层面追踪到泄密源。

■ 解决方案

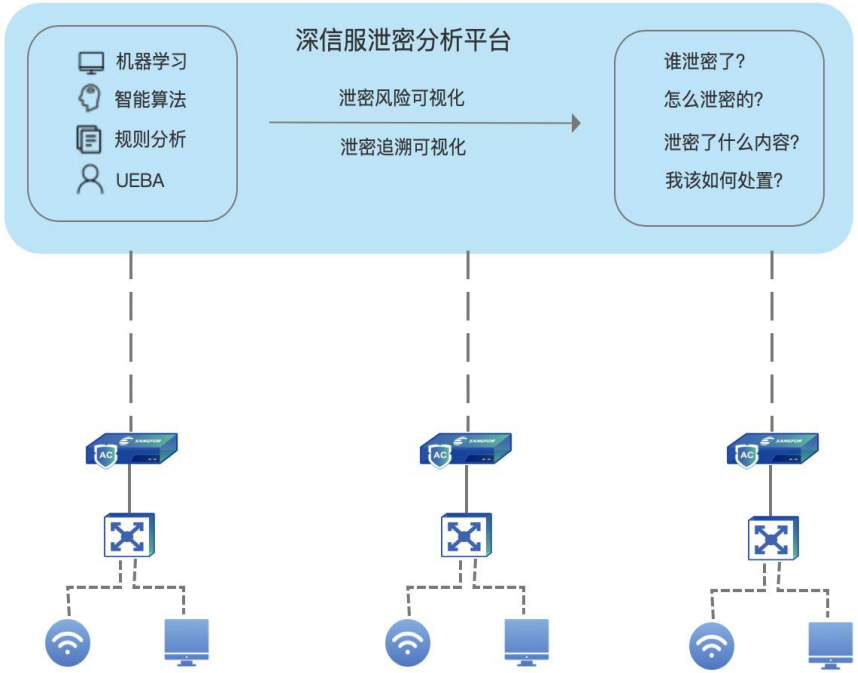
1、通过集中管理部署方案，在总部和各个分支机构的网络出口部署AC，采集各个地区的上网数据。

2、将AC采集的数据汇总到总部内部威胁管理平台，同时，DLA平台采用了集群部署的模式提高处理性能。

■ 方案价值

- ✓ 1、完善防御：全集团陆海空立体防御体系中，已部署终端防泄密，需要继续部署网络防泄密，实现网关通道数据泄密的追踪分析，尤其是QQ/微信、邮件、网盘、云笔记的外发数据追踪分析。
- ✓ 2、数据审计：强大的文件识别引擎，可帮助安全管理人员掌握所有外发数据的概况，包含文件或消息总数，数据类型（客户信息、财务数据、设计图纸等），外发通路等，并支持留存以满足网安法的要求。
- ✓ 3、泄密分析：系统内置多行业泄密规则，可自定义适合企业的泄密检测规则，可从行为及场景的分析角度提高泄密分析准确性，并支持AI泄密分析。最终将所有结果汇聚到人的维度，并支持分级管理，大大降低了安全管理员的工作量。
- ✓ 4、泄密追溯：支持多种追溯模式，可根据关键字、段落或文件追溯到泄密员工，支持doc、ppt、xlsx等文档内容泄密追溯，支持追溯压缩包内容追溯，支持截屏抗抵赖。同时，强大的追溯能力也能对泄密行为起到一定的震慑作用。

【企业】金发科技



金发科技是国内产品最齐全、产量最大的改性塑料生产企业，总部位于广州科学城，旗下拥有46家子公司，在南亚、北美、欧洲等海外地区设有研发和生产基地，产品远销全球130多个国家和地区，为全球1000多家知名企业提供服务。金发科技的产品以自主创新开发为主，覆盖了五大类自主知识产权产品。

客户属于典型制造业客户，内部有很多图纸和技术资料，对防泄密诉求比较强烈，管理层要求要做防泄密方案。前期已经部署加密解密式终端防泄密方案。

■ 需求与挑战

客户希望在已有终端防泄密的基础上补充更易推广、更全面的防泄密方案，解决需求痛点，实现全员防泄密。

- 终端防泄密方案过重，用户有明显感知，且配置部署周期长，运维成本较大，不适合大规模推广，所以对研发部门以外的员工不太实用。
- 公司内部发现有员工通过IM聊天工具外发一些公司的内部资料，希望加强对网络应用的管控，终端防泄密方案的网络审计效果不足。
- 公司希望整体建设体现全面的防泄密效果，终端防泄密方案注重事中的阻断、加密，对事前的风险预警、事后的快速追溯支持不足。
- 在使用终端防泄密的过程中，有很多人都开放了解密的权限，导致加密解密的方案也没有用起来，方案管理难。

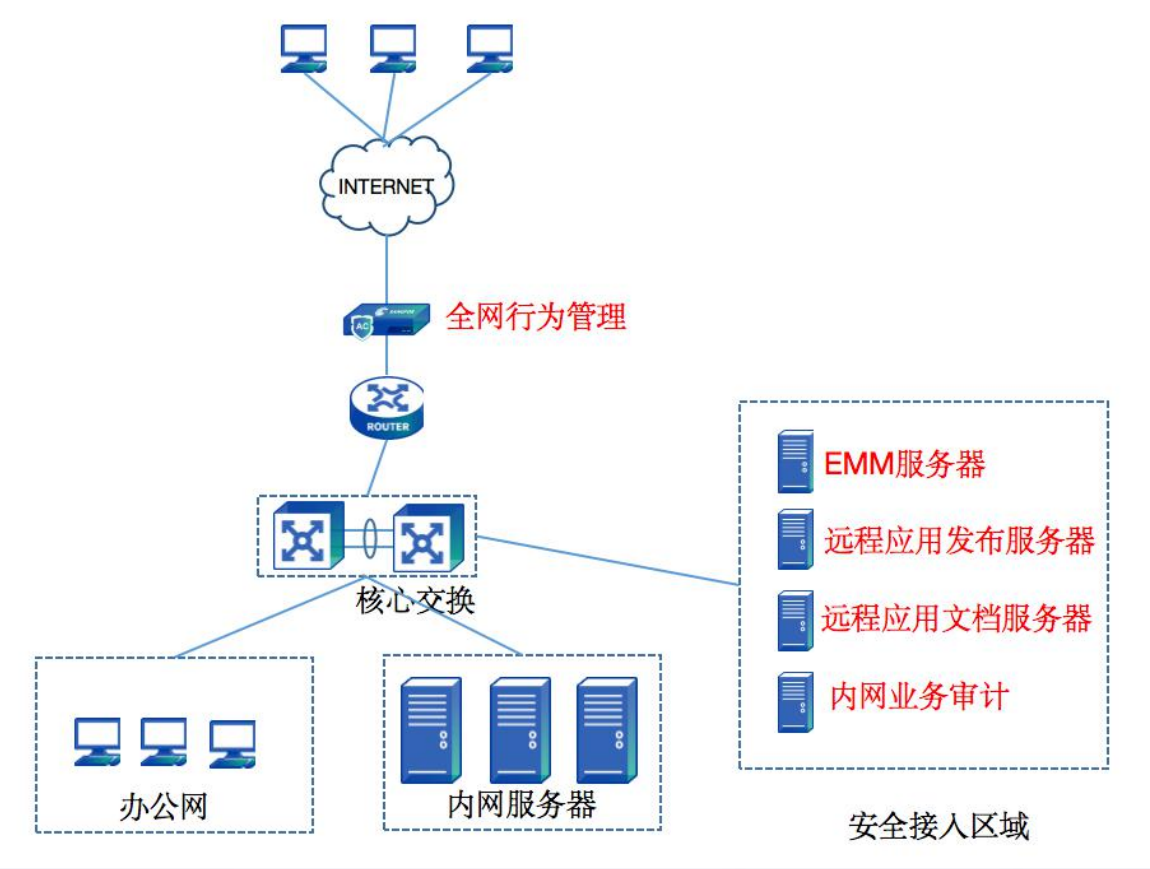
■ 解决方案

我们为客户提供的方案是每个分支上1台上网行为管理，分别审计各分支的上网行为。总部分支通过专线打通，分支的上网行为日志通过专线汇总到防泄密分析平台DLA上，在DLA平台统一做数据分析和汇总处理，解决客户全员防泄密的诉求

■ 方案价值

- ✓ 1.结合桌面云联合做隔离+网络侧防泄密：传统的终端防泄密存在短板，难以完全满足客户需求，例如后期由于内部解密权限控制没有做好，现在很多人都可以做文件的解密外发。在本次项目优化后，目前通过给研发侧上桌面云来做双网隔离，其他员工通过AC+DLA方案管控，AD域推送准入插件来做IM聊天内容的审计和附件的审计，补齐没有部署桌面云的员工泄密场景。
- ✓ 2.构建总部-分支的防泄密整体方案：客户有6个分公司，通过在每个分支部署AC审计网络行为日志，并通过专线来把上网行为日志传到总部进行泄密分析，一套系统实现了全员防泄密，并可以通过统一平台进行管理，覆盖全面，运维简单。

【企业】广州市交通投资集团有限公司



广东省交通集团有限公司是经广东省委、省政府批准组建的大型国有资产授权经营有限责任公司，2000年6月挂牌成立，主要经营高速公路的投资建设与经营，汽车客货运输、公路设计施工监理、智能交通等业务。

■ 需求与挑战

交通集团下属公交集团发生信息泄漏事件，某员工通过OA系统将重要文件下载至本地，再通过微信朋友圈进行传播，造成了非常不好的社会影响。事件发生后，公交集团重新梳理日常信息管理和保护方便面存在的薄弱环节，整改加强并落实数据的保护工作，保证敏感数据不再被泄漏。

1、集团自身数据安全需求：重要数据文件防泄密，避免再一次出现泄密事件的发生

2、网络安全法需求：网络安全法明确要求网络运营者对网络数据具有防止其被篡改、泄密的义务和责任。

3、等级保护要求：网络运营者应按照网络安全等级保护的要求，保障网络免受干扰，防止网络数据泄露或被窃取、篡改。

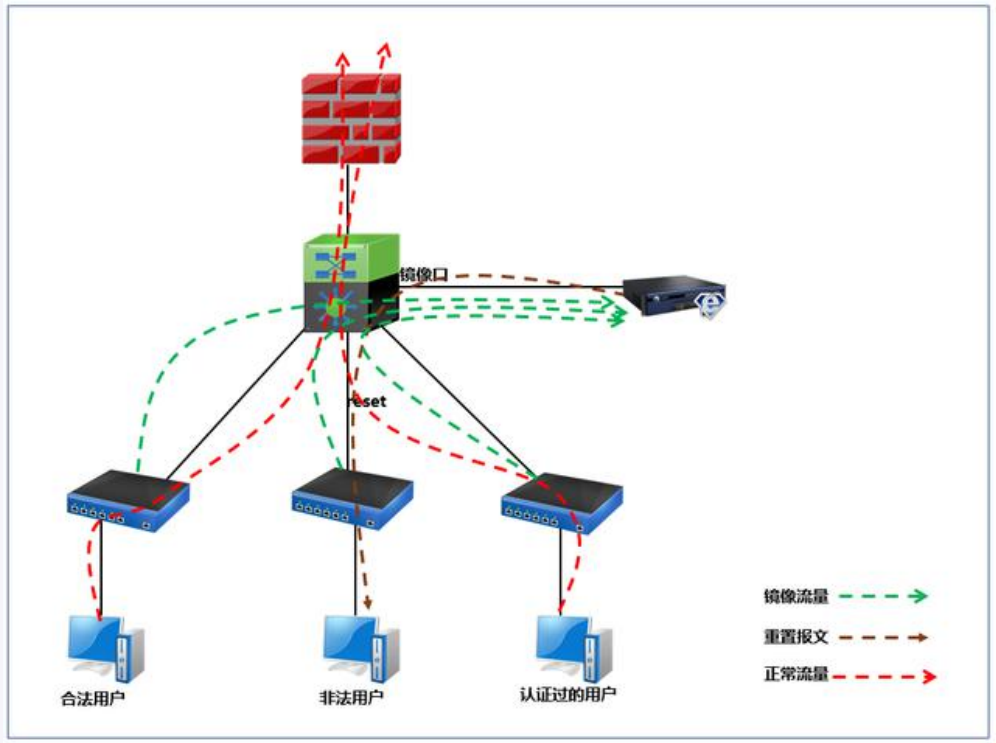
■ 解决方案

通过在公司出口串联及核心交换机旁路部署深信服全网行为管理，采用802.1X的协议结合深信服终端准入插件，实现内部终端入网前、入网中、入网后全面管控和审计

■ 方案价值

- ✓ 入网前：通过终端安全插件对终端弱密码、未安装杀毒软件、注册表不全、高危端口开放等脆弱性进行检查，确保终端自身安全性
- ✓ 入网中：通过准入控制模块，以多种认证方式对有线、无线终端进行统一认证，确保终端是正确的用户在使用
- ✓ 入网后：通过出口+核心旁路的全网行为管理，对无论是访问内网还是访问互联网的行为均可实现审计和管控

【金融】徽商银行



徽商银行于2005年12月28日正式成立，总部设在合肥，由安徽省内6家城市商业银行和7家城市信用社联合重组设立。徽商银行是以资产、贷款、存款规模计算的中国中部地区最大的城市商业银行。目前拥有199个机构，覆盖安徽全部16个省辖市以及邻近的南京市。

■ 需求与挑战

目前整个开发区域分为办公区和服务器区，通过专线连接生产网络，目前的生产网络主要承载了客服系统和集中运营系统等关键生产业务系统，现有的网络结构对于四个汇聚下联的办公区没有专用的网络安全设备实现对于终端接入的准入控制，势必会存在一定的安全隐患。总体需求分析如下：

1、实现对于终端接入的准入控制，外来非法终端或不在绑定列表内的用户无法访问内部资源。

2、希望整个方案不改变现有的网络拓扑，且后期运维方面要采用统一的认证方式。

3、不能采用在客户端安装插件，或者安装客户端的方式。

结合以上需求，整个设计需要一种既能做到可信接入内网，又能对终端进行有效检测，减少终端运维成本的方案。

■ 解决方案

在网络中转交换机上旁挂部署内网安全准入控制设备，为提供整个设计的可靠性，采用双机模式，通过四根线缆连接，两根作为设备的管理口，两根作为接收流量的镜像口，同时在中转交换机下联的四个汇聚交换机上做远程镜像，将内网办公业务的流量镜像到内网安全准入设备上。

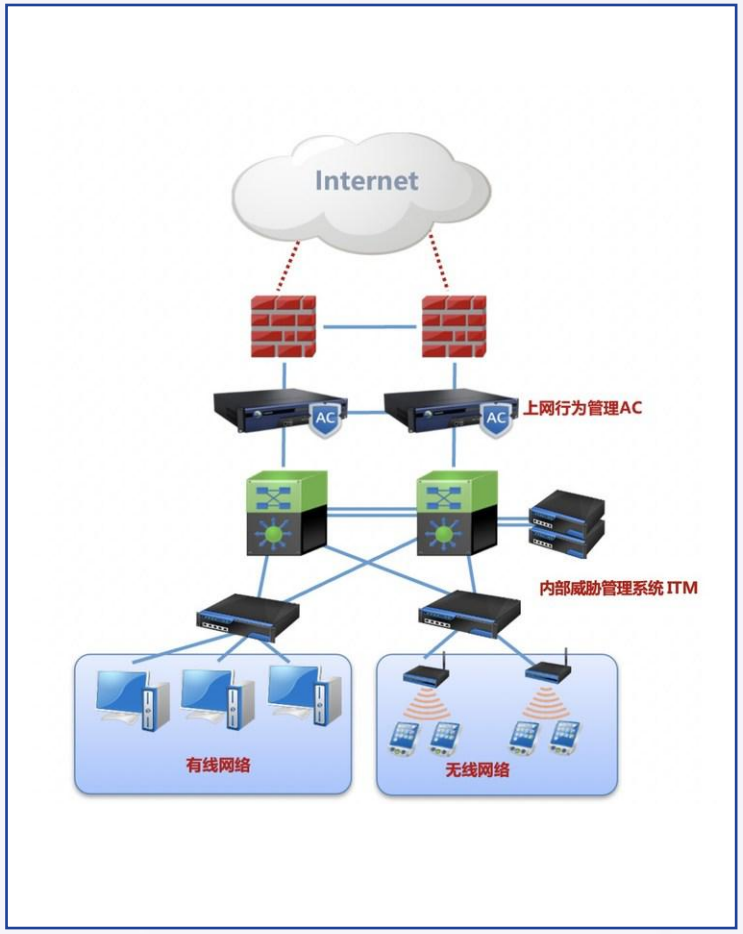
■ 方案价值

1、 实现终端安全准入：采用现有的IP+MAC地址的方式实现对于终端合法性的检测，不在绑定列表内的用户无法访问内部资源，新用户进入待审批小组，管理员通过审批功能实现轻松管理。

2、部署方便、运维简单：整个方案不改变现有的网络拓扑，只需要旁路部署，即使设备宕机，也不影响客户网络，后期运维方面要采用统一认证方式，不采用802.1x方式实现准入。

3、客户端无感知：客户端无需安装插件和客户端，上线安全准入，用户无感知，大大降低科技部门沟通协调难度。目前总行部署4台，后期各地市分行也将进行部署，实现内网终端的安全准入；

【金融】招商信诺-数据泄密管控



招商信诺人寿保险有限公司是由两家信誉卓著的百年名企共同出资创立的中美合资寿险公司。在国内拥有超过500家公立及私立直付医疗机构，与信诺全球超过100万间国际医护中心紧密合作。2008、2009年，招商信诺连续两年被《金融时报》与中国社科院金融研究所评为"最佳外资人身（寿）保险公司"

■ 需求与挑战

招商信诺是互联网平台型的保险公司，职场办公人员较多，内部有自己的产品开发团队，很多业务开展都是在线上进行的，内部员工经常会接触到一些客户敏感信息，对防泄密诉求比较强烈，已部署部分赛门铁克防泄密方案，但方案比较重，担心广泛推广后，影响用户端的使用体验，经过客户内部反复考虑，最终选择深信服内部威胁管理平台ITM做招商信诺网络侧的防泄密建设。

整体需求梳理后如下：

1、需要轻量易落地的防泄密方案，部署和运维成本可控
2、希望加强对网络应用和图片泄密途径的管控和审计
3、需要可视化的防泄密风险预警和事后快速追溯能力

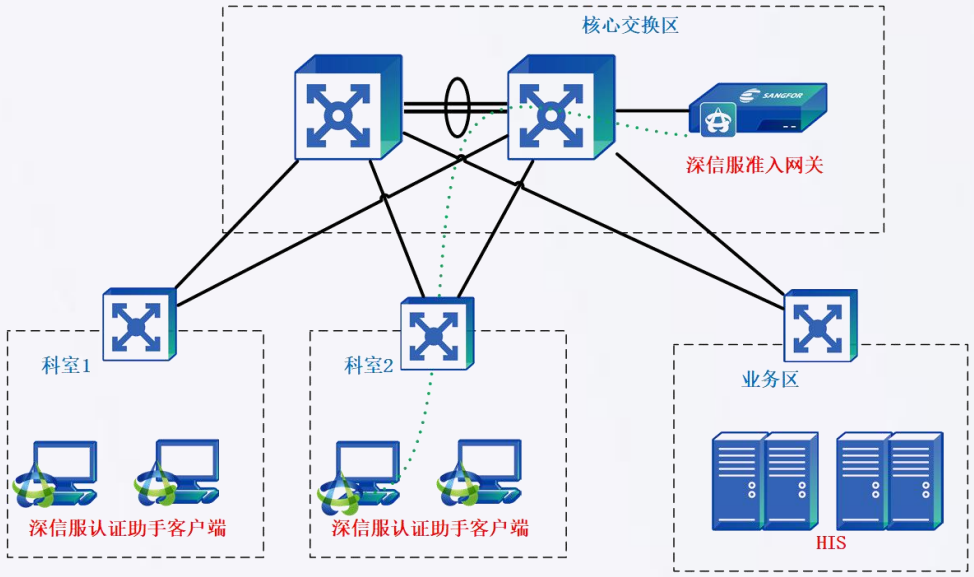
■ 解决方案

本项目在深圳总部机房部署全网行为管理AC和内部威胁管理系统ITM，通过全网行为管理对终端入网、用户内网访问行为、用户泄密行为进行审计，之后将数据汇集到内部威胁管理系统ITM之中，通过ITM建立用户业务访问模型，做到对防泄密行为事前发现、事中阻断、事后溯源的全生命周期管理。

■ 方案价值

- ✓ 管控范围全：该方案部署简单，结合客户原有DLP，以终端审计+网络审计的模式满足大多数场景需求
- ✓ 用户端体验好：优先做审计与追溯从而尽可能降低对终端用户的影响
- ✓ 功能全面：支持IM审计、https全审计、U盘审计、图片OCR识别、智能风险识别、多方式泄密追溯
- ✓ 性价比高：在做防泄密的同时可实现上网行为管控

【医疗】石家庄市第一医院



石家庄市第一医院是一所综合性三级甲等医院。拥有床位700张，职工960余人。年门诊量30万人次，年收治病人14000人次，年手术3480台次。2003年全年业务收入1.3亿元。在等级保护建设中，重点关注全院2500台PC的安全基线和网络准入建设。且需要考虑医生的实际操作体验。

■ 需求与挑战

- ✓ 等保三级边界完整性规范：医院按规定需满足等保2.0规范，需要对全网终端实施接入认证和非法外联管控。
- ✓ 医院办公终端U盘管控：为了保障办公终端安全运行，医院IT管理员希望禁止专用PC使用U盘，防止接入带病毒的U盘而造成主机失陷。
- ✓ 医院办公终端入网管理：客户本地共有约2000台办公PC，包括医生/护士办公终端、医疗器械服务终端、自助办理业务终端等，这些专用PC主要连接本地内网和医疗专网，如果出现安全问题可能给医院业务稳定性造成极大的安全隐患。客户希望加强对内网办公PC的安全管理，重点防止专用PC擅自连接热点、使用4G网卡等方式访问互联网，避免因为访问恶意链接、下载木马文件等造成主机中毒。

■ 解决方案

1.业务安全准入：AC单臂旁路部署（不做镜像），与核心交换机做portal认证对接，因采用C/S架构的HIS系统，所以采用认证助手客户端作为入网登陆入口。为方便医生操作，准入认证通过自动后台认证进行，无需医生操作。

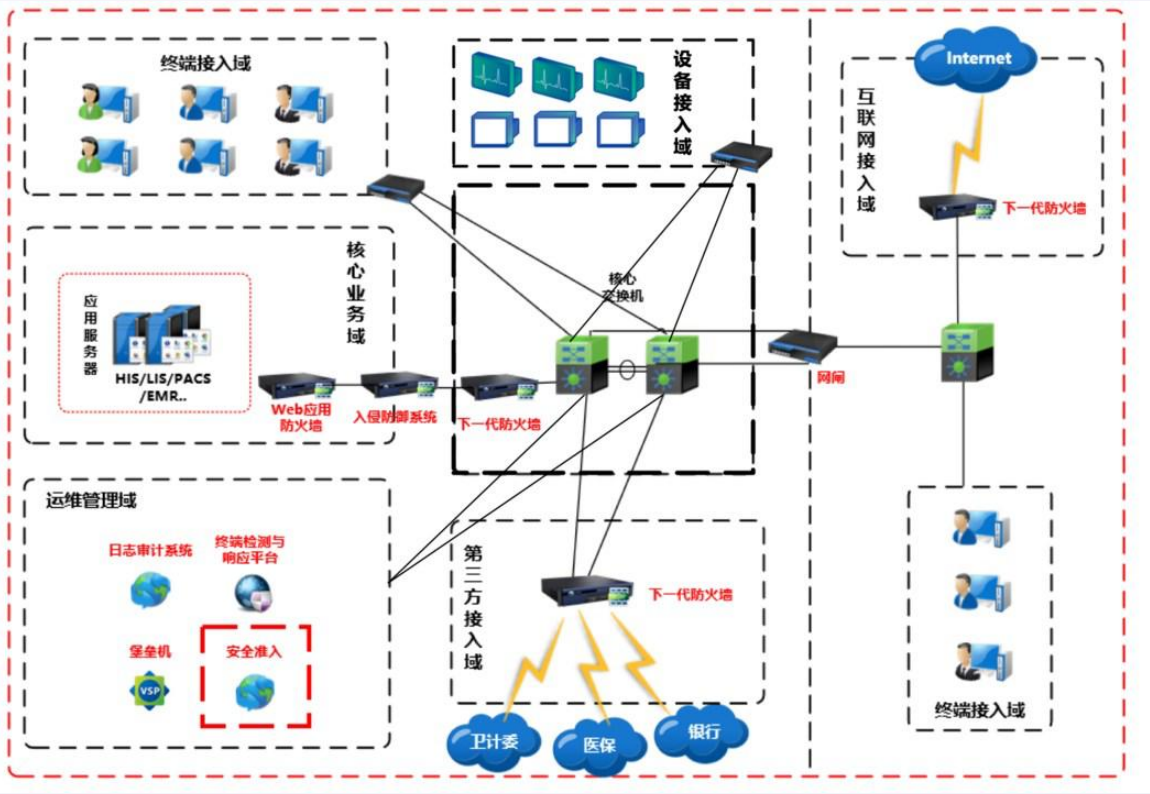
2.外联管控：同时，AC对入网PC推送安全插件，实施非法外联管控，可对外联行为进行检测和阻断，防止非法路径暴露内网导致的网络攻击，并满足等级保护要求。

3.U盘使用管控：AC通过终端插件实现对指定PC下发U盘管控策略，规避不安全U盘接入内网终端。

■ 方案价值

- ✓ 终端安全基线检测：对全网2500台PC进行合规性检查，包括防病毒软件安装、运行、操作系统版本、补丁情况、注册表键值、终端程序运行情况等，对不合规项进行推送修复。
- ✓ 精细U盘管控：支持U盘接入告警/可读/可读写/拒绝 4种管控类型，可配置黑白名单。
- ✓ 定向访问控制：通过下发对应的目的IP白名单/黑名单给终端，在终端层面严格控制其能访问的资源，保障精准的访问控制策略。

【医疗】湖南省沅陵人民医院



湖南省沅陵县人民医院坐落于沅陵辰州东街的沅水河畔，与名胜风景区凤凰山隔河相望。是一所享誉湘西，融医疗、教学、科研、预防、保健为一体的公立二级甲等综合性医院，坚持以区域内一流的人才、一流的技术、一流的设备、一流的服务造福广大患者。

■ 需求与挑战

1、医院办公终端防非法外联：重点防止专用PC通过擅自连接热点、使用4G网卡等方式访问互联网，避免因为访问恶意链接、下载木马文件等造成主机中毒。

2、医院办公终端U盘管控：同样出于办公终端安全运行的要求，医院IT管理员希望禁止专用PC使用U盘，防止因为接入带木马蠕虫等病毒的U盘而造成主机失陷。

3、等保三级边界完整性规范：医院按规定需满足等保2.0规范，需要对全网终端实施接入认证和非法外联管控。

■ 解决方案

湖南省沅陵县人民医院在业务区和接入区汇聚的核心交换机旁路部署全网行为管理，实现终端接入/外联管控、终端安全防护加强、业务访问权限控制。

■ 方案价值

- ✓ 二层安全准入：结合二层交换机做802.1x认证，用户信息源导入，同时做安全基线检测；对于哑终端类型的设备采集固有信息，统一策略检验合法后才放通入网。
- ✓ 非法外联管控：：实施非法外联管控（包括：拨号行为、双网卡行为、有无线行为、连接非法WIFI、私接4G网卡、使用非法网关、连接外网等），防止非法路径暴露内网导致的网络攻击，并满足等级保护要求。
- ✓ U盘使用管控：支持灵活告警/可读/可读写/拒绝 4种管控类型，规避不安全U盘/存储设备接入内网终端；对于临时U盘使用需求，白名单放通。