SANGFOR
深信服科技

深信服产品线全家福

深信服 广东区产品运营专家部
熊文韬（186-6567-8559）

公司概况

关于深信服

SANGFOR

深信服科技股份有限公司是一家专注于企业级安全、云计算及基础架构的产品、服务和解决方案供应商。在如今的数字化时代，公司立志于承载各行业用户数字化转型过程中的基石性工作，从而让各行业用户的IT更简单、更安全、更有价值。

全球50多个办事处

员工数量 6500+

40%研发　20%服务
30%市场　10%其他

4大研发中心
硅谷、北京、深圳、长沙

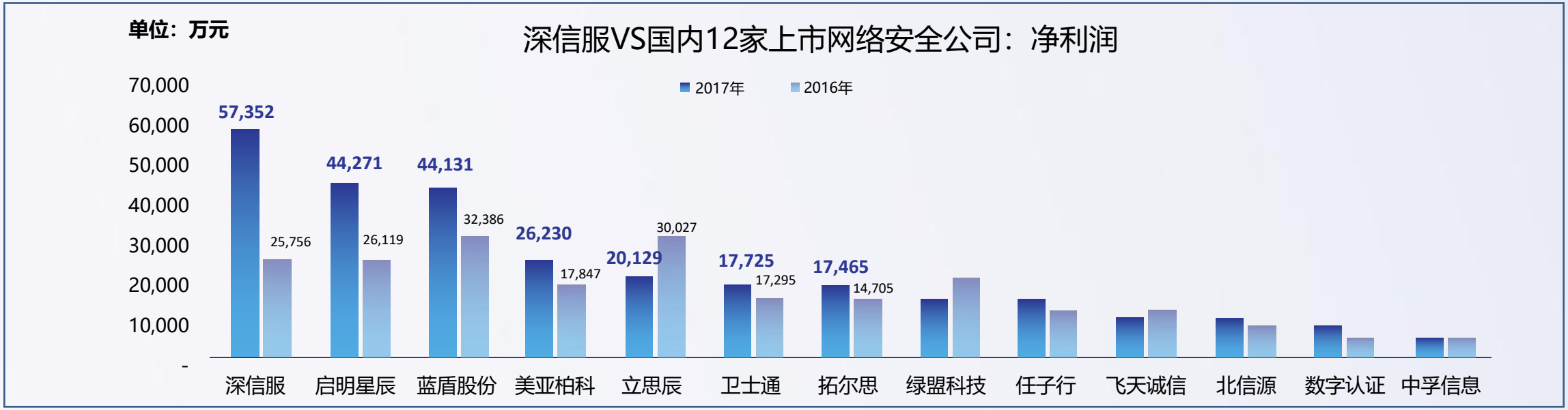
3大CTI
长沙 、深圳 、吉隆坡

深信服科技简介-集团发展历程

SANGFOR 深信服科技

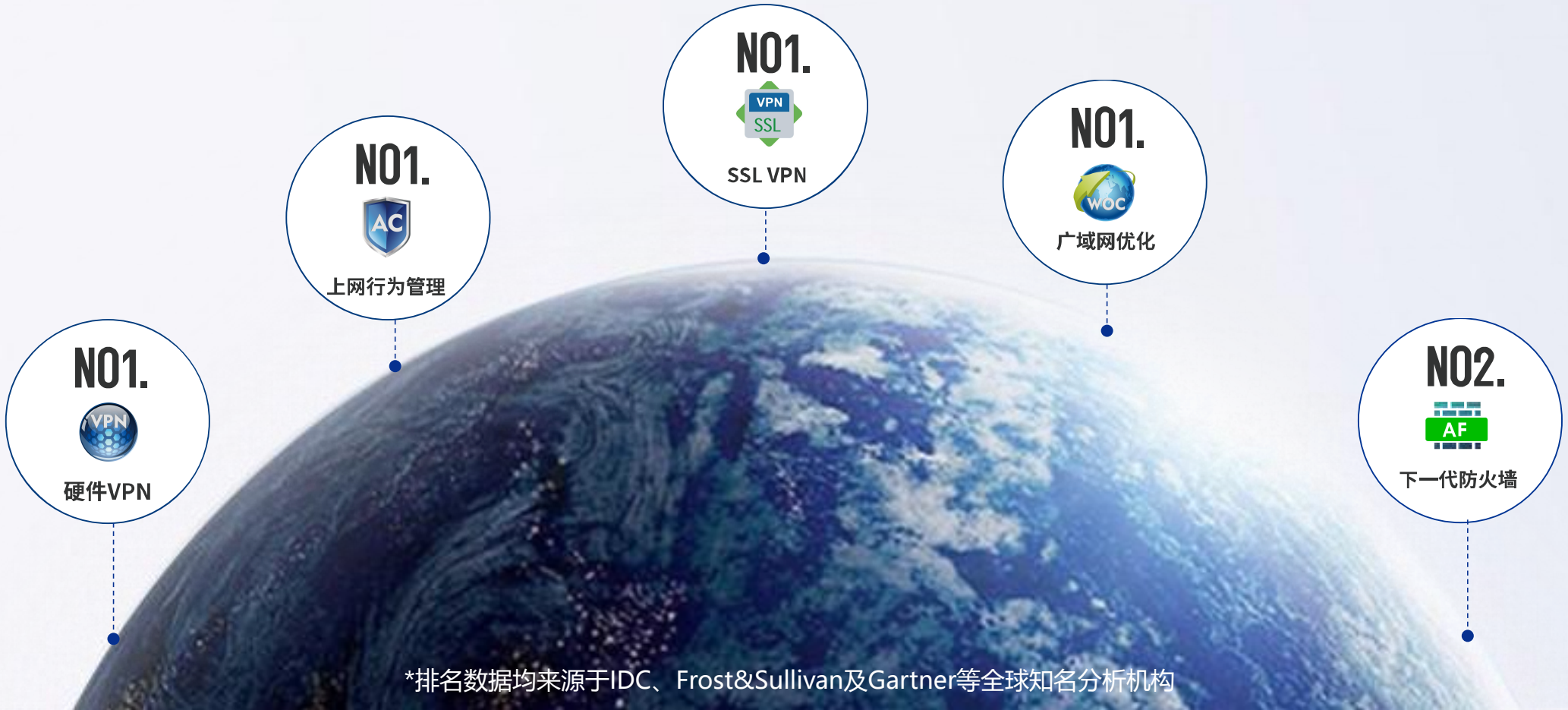
*以下数据均指合同销售额

深信服科技简介-规模最大



深信服科技简介-中国企业级安全领导者

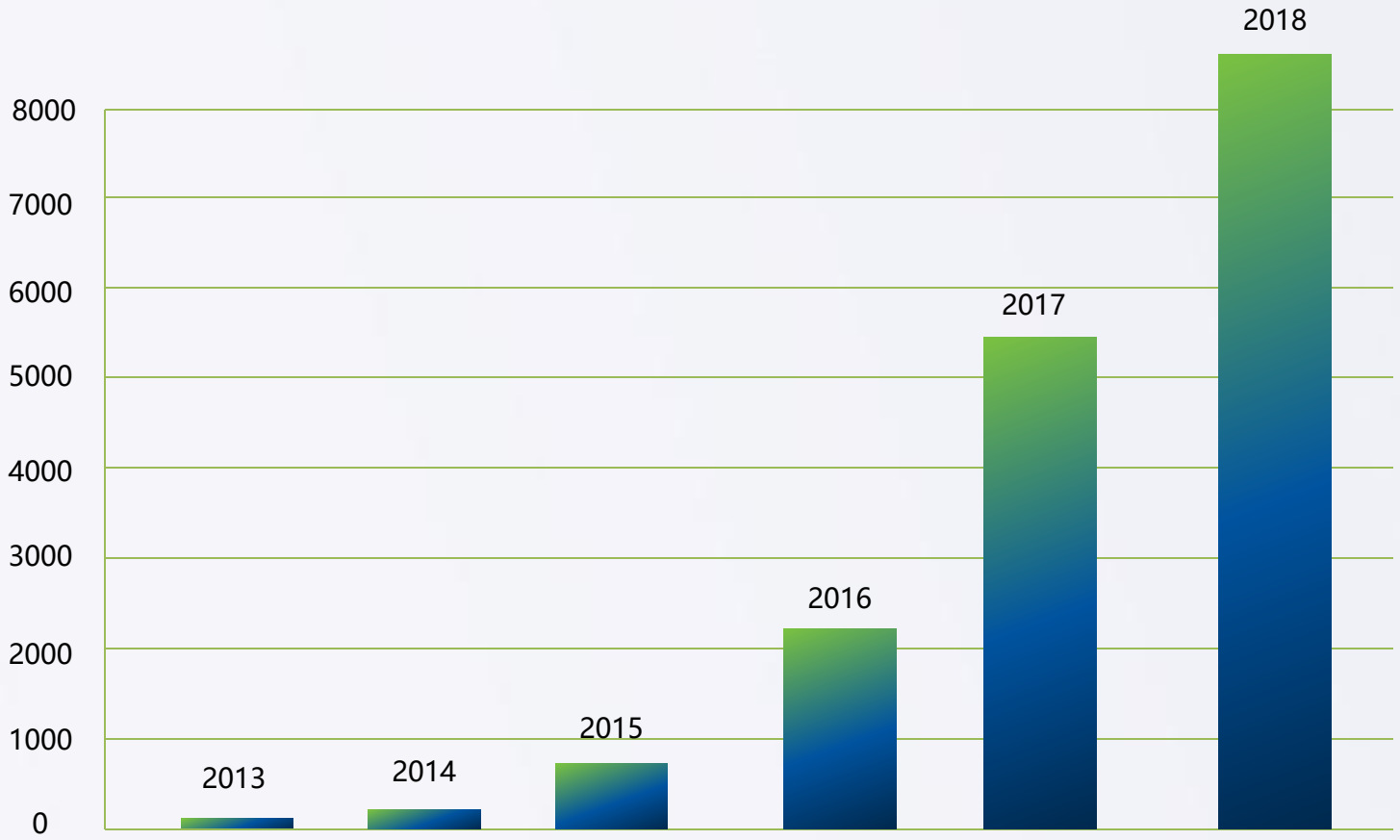
多款安全产品市场占有率第一



*排名数据均来源于IDC、Frost&Sullivan及Gartner等全球知名分析机构

云计算业务复合增长率100%+

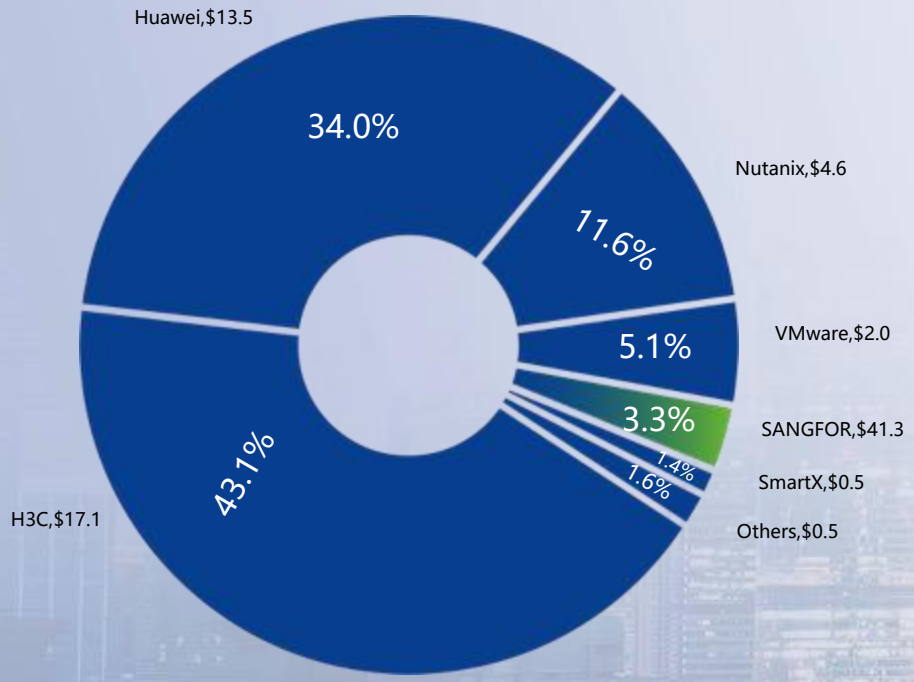
2013-2018年深信服云计算业务营业收入一览表



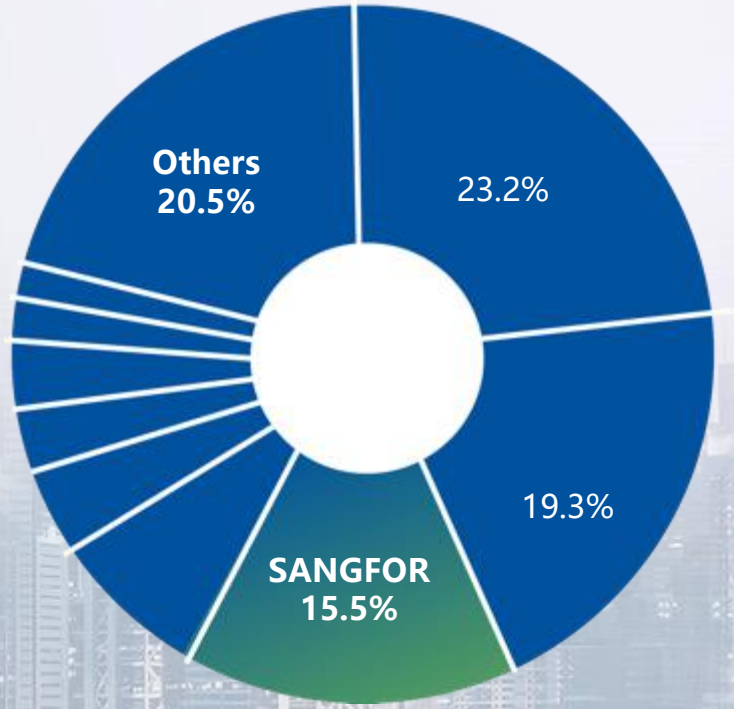
100%+

过去3年复合增长率

超融合占有率自2016年开始稳居市场前三



超融合中国区市场占有率（2015H1）
份额（%），销售额（百万美元）



超融合软硬件整体中国区市场占有率
(2018，IDC)

软件定义的基础架构

桌面云

- 中国桌面云市场占有率第二
- 累计75万云桌面授权
- 1000台以上大规模云终端部署案例100+

应用交付

- 国内唯一连续5年进入Gartner魔力象限
- 连续5年市场占有率第一的中国品牌
- 入围中国移动集采

SD-WAN

- 国内首家获可信云•SD-WAN解决方案产品型认证
- 荣获2018中国SD-WAN峰会优秀应用评选“优秀应用奖”

SANGFOR
深信服科技

深信服产品体系总览

SANGFOR 深信服科技

深信服产品线体系

云	安全云脑	云图X-Central	SaaS化服务（云眼、云盾）	
网	下一代防火墙 AF	WEB防护系统 WAF	SSL VPN	
	入侵防御系统IPS	上网行为管理 AC	云安全资源池平台	
端	终端检测响应EDR	企业移动管理 EMM	数据库审计 DAS	桌面云aDesk	口袋助理
基础网络	广域网 SD - WAN	安视交换机		
数据中心	云计算aCloud	企业级分布式存储EDS	应用交付AD	
合规类产品	等保一体机	日志审计	堡垒机	

运营管理

- 安全感知平台 SIP
- 行为感知平台 BA
- 集中管理平台 BBC
- 安全服务

SANGFOR
深信服科技

一. 深信服产品系概述

二. 云端安全产品介绍

三. 网络安全产品介绍

四. 终端系列产品介绍

五. 基础网络产品介绍

六. 数据中心产品介绍

七. 安全合规产品介绍

八. 运营管理产品介绍

九. 产品推广工具介绍

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

安全云脑

深信服安全云脑

构建平台级下一代安全能力核心

深信服安全设备

厂商安全情报

全网安全信息

攻防专家

安全分析师

数据科学院

安全云脑

- 自主进化架构
- 多引擎分析
- 全面数据支撑
- 庞大算法资源池
- 人工智能大数据

黑客画像

威胁分析

攻击溯源

联动处置

文件云查

安全能力

流量签名

战术情报

病毒指纹

……

产品化交付


下一代防火墙


安全态势感知


SSL VPN


上网行为管理


终端安全EDR


安全资源池


aBos一体机

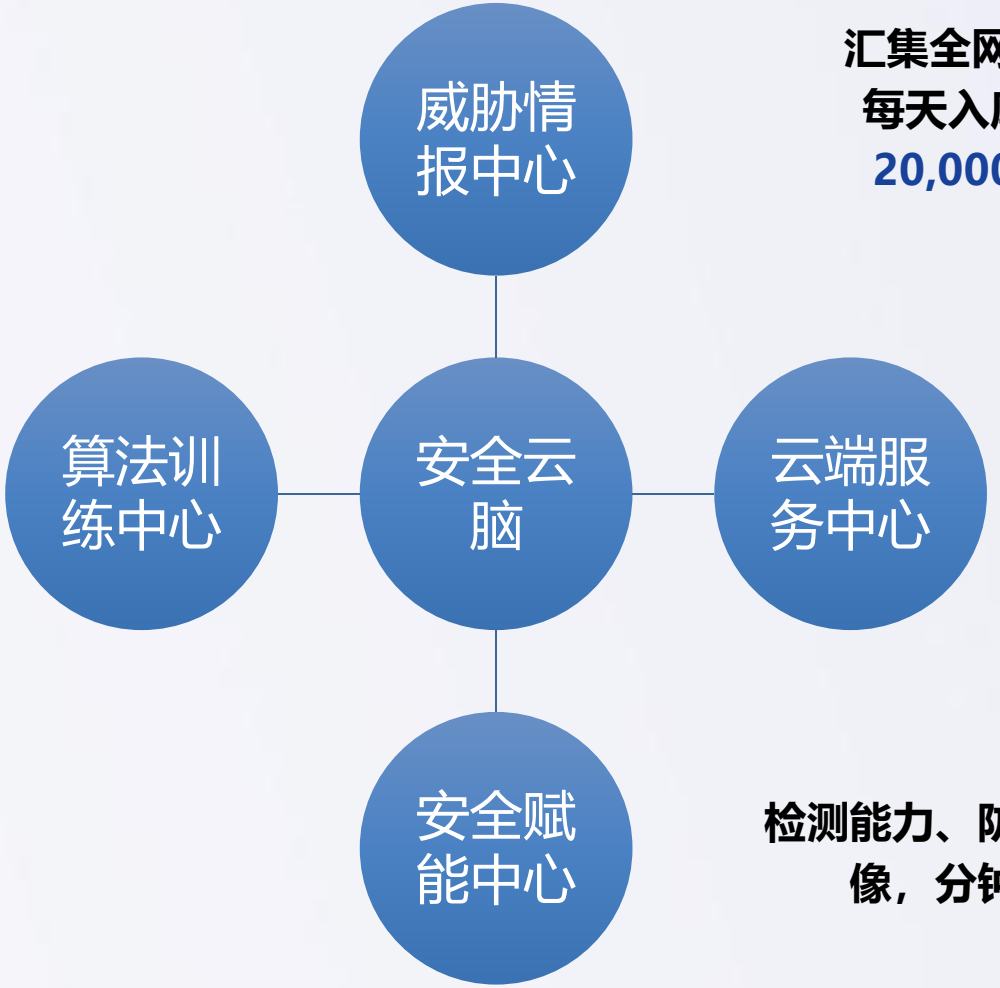
能力化交付

安全威胁情报	异常文件识别	安全分析能力
未知威胁防护	告警信息推送	安全设备联动

服务化交付

云守　云眼　云盾　云镜

安全云脑的功能角色——深信服安全能力中心



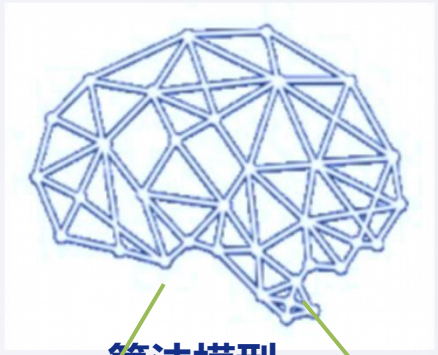
汇集全网威胁情报，大数据高效存储分析
每天入库：30,000+病毒、文件样本，
20,000+恶意域名，5,000+恶意链接

算法资源池，100+机器学习
算法高效训练调优

安全事件云端快速处置，
关键业务外部事件监测

检测能力、防御能力、威胁画像，分钟级快速下发

客户价值



最新
威胁情报

算法模型
规则
特征

云端
监测防御

运维处置专家
攻防专家
安全分析师

最新威胁防御识别

APT、未知威胁防御识别

外部事件监测
云端流量清洗

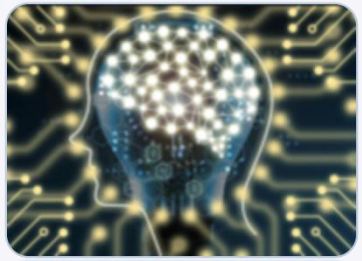
远程运维
快速问题处置

安全云脑背后的专家团队

深信服
创新研究院

安全、云计算前沿技术孵化中心

博士30+以上，来自耶鲁大学、北京大学、清华大学、香港科技大学、瑞士洛桑联邦理工学院、上海交通大学、中国科技大学等国内外一流高校



安全云脑团队

- 云脑架构设计
- 演进规划
- 策略调优，管理运维

雪豹安全攻坚队

- 安全检测技术攻关
- 人工智能模型构建
- 威胁情报搜集和利用

千里目安全实验室

- 攻防技术攻关
- 未知漏洞研究挖掘
- 新型防御技术突破

凤凰架构团队

- 云计算新技术突破
- 算法、架构性能优化
- 智能资源调度

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

云图X-Central

信服云图

统一可视化云端管理平台

深信服云图（Sangfor X-Central）通过打造一个架构开放一站式、多元化，打通所有深信服线下盒子和线上云服务的平台，客户在统一平台上实现对深信服所有的网络设备、端点防护和云安全应用的统一可视化管理，一站式集中展示安全风险、处置和批量管理设备策略，为客户提供能全面管理所有深信产品应对各类安全威胁整体解决方案，从而降低客户安全管理复杂度。

以法律法规、安全标准为基线：网络安全法、等级保护、ISO27001、关键信息基础设施安全保护条例……

云图功能介绍

多产品统一管理

对深信服所有的网络设备(AC/AF/aBOS/WOC/MIG)、端点防护(EDR)和云安全应用(云眼/云盾/云镜)的统一管理

智能监控

首页大屏包括：安全状态大屏、分支状态大屏、VPN状态大屏，监控企业风险，监控内容包括上下行流量，带宽利用率等关键参数

智能告警

安全风险事件告警、网络告警、分支离线、授权告警、资源告警，五维度告警

分支设备统一管理

网络设备配置统一下发
软件版本库实时更新
分支设备易部署，快速上线
远程接入分支设备

集中查看和处置安全风险

收集设备/安全服务的安全日志、配置等，展示企业内业务服务器/终端用户存在的安全风险

VPN统一管理

VPN拓扑管理、VPN设备概览、智能选路策略配置

技术优势

运维更便捷

在单一平台上做到对深信服所有的网络设备统一管理和可视化

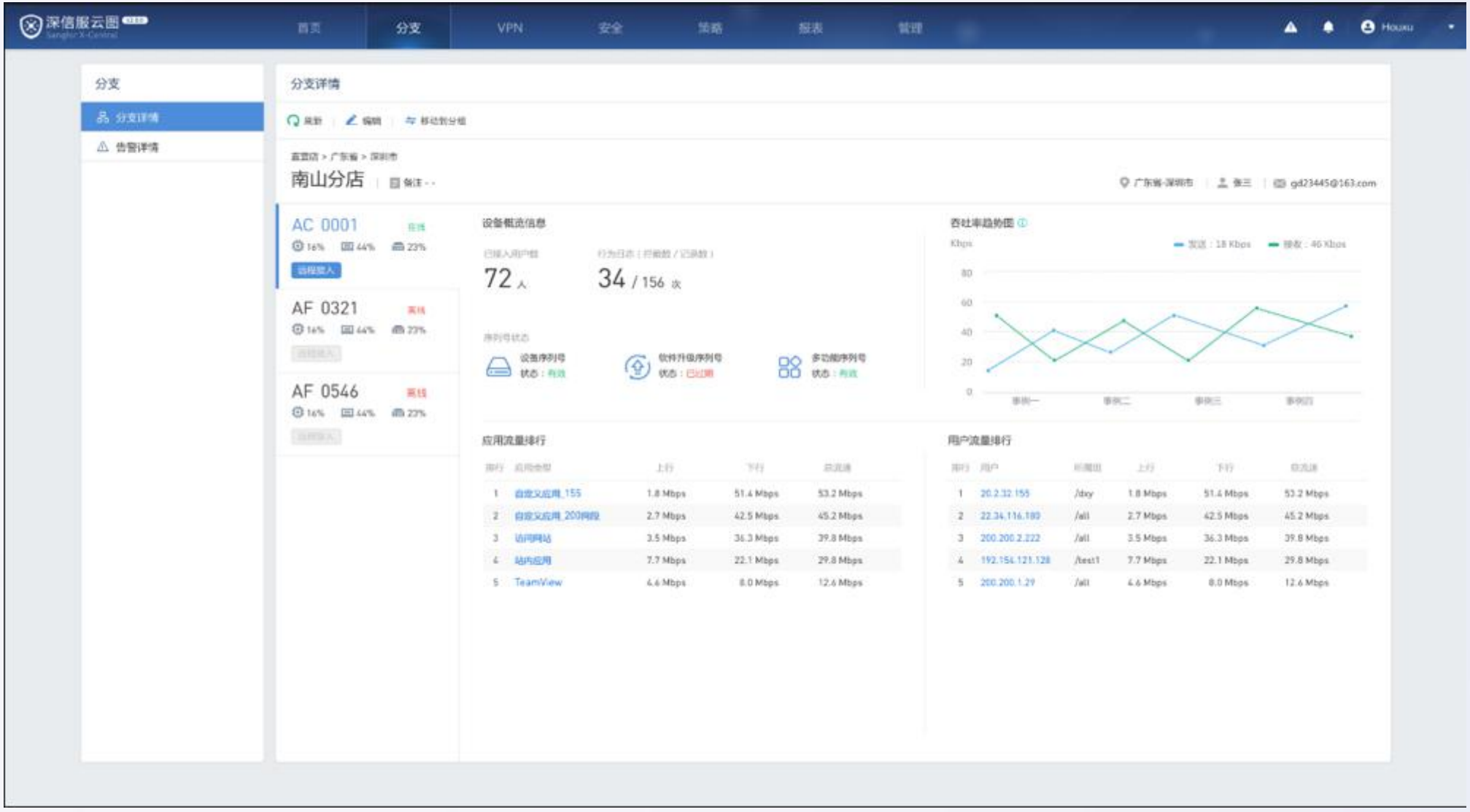
管理更全面

不不仅仅是个运维管理中心，通过该平台还可以对集团分支进行智能管理；以及对VPN远程接入情况进行管理

技术优势

SANGFOR 深信服科技

分支-智能监控



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

SaaS化服务——信服云盾

信服云盾

深信服利用云计算技术融合评估、防护、监测和响应四个模块，打造由多引擎智能驱动，围绕业务生命周期，深入黑客攻击过程的自适应安全防护平台，帮助用户全面代管业务安全问题，交付全程可视的安全服务。

主动评估风险，防患于未然

分布式扫描系统在业务上线时会对业务进行一次全面评估，同时每天监测业务变化情况，分析引入的新风险问题，实现对风险变化的快速感知。

还原攻击行为，联动防护

基于黑客攻击过程的完整WEB系统安全防护，通过威胁情报共享机制全球联动封锁攻击源，有效避免出现第二个受害者。

实时监测，在线响应

对安全事件进行7*24H的全面监测，实现分钟级发现篡改、网马、黑链等安全事件，并及时在线进行响应处置，通过微信告知用户。

云盾服务类别及内容说明

服务类别	服务名称	服务专家	全程可视
基础防护	Web应用安全防护 入侵防护 DDoS/CC攻击防护 独享防护 防绕过 失陷监测 安全可视化	千里目实验室 防御专家 处置专家	风险评估报告 安全事件报告 每日值守报告 每月运营报告 业务风险大屏展示 防御过程在线展示 防御结果在线展示
高级防护	动态防护 定向防护 实时对抗 应急对抗		
评估/监测	漏洞脆弱性检测 实时漏洞检测 高危0day事件告警 业务可用性监测 篡改监测		

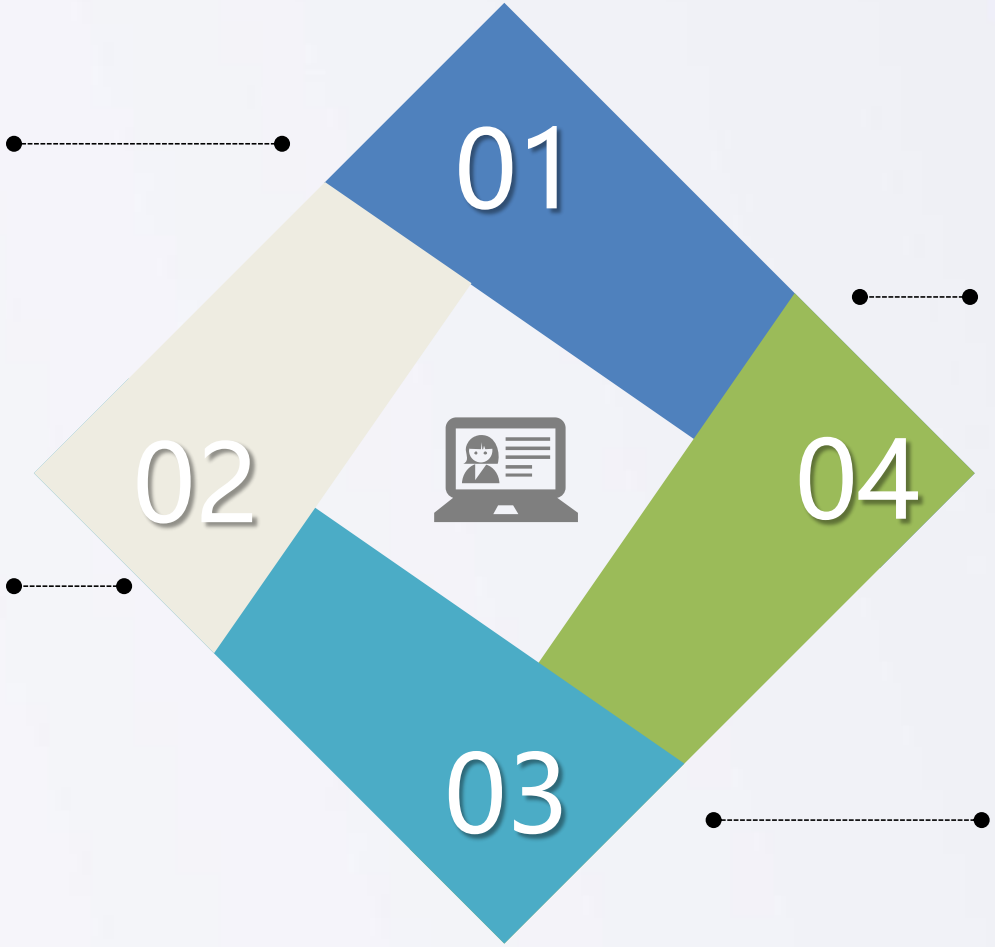
技术优势

防御模块独享

采用超融合云计算平台，利用网络功能虚拟化技术，给
每位用户一套独享防护模块，实现专属防护。

自适应安全

融合持续评估、联动防护和实时监测的安全能力，实时
应对风险、攻击和事件的变化，突破服务周期性问题。



专家代管

集合千里目实验室，防御专家和处置专家在线全程运维，具备业界更好的安全代管能力。

全程可视

以全程可视化的交付方式让用户全面掌握业务风险，防护过程和防护结果。微信端预警效果展示服务过程可视化，掌握业务安全。

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

SaaS化服务——信服云眼

信服云眼-网站云监测&网站云防护

信服云眼为互联网业务提供持续的风险评估+实时监测+篡改处置+应急对抗服务，让用户重新获得更加安全的保障

持续评估

- ✓ 新业务上线，24H内进行全面的上线评估，包括暴露面，脆弱性，内容安全，并作为基线，每天持续复查；同时每天对资产变化进行监测，持续分析新增资产引入的风险情况。

实时监测

- ✓ 实时监测页面篡改、0day、网马、黑链、DNS和可用性等安全事件，并生成可视化报告及时通知用户，让用户可以实时掌握安全状况，争取宝贵的处置时间。截止目前，我们累计为50万多个网站继续拧了安全监测，监测网页数量接近17亿；

篡改处置

- ✓ 实时监测页面状态，通过大数据分析技术分钟级发现页面是否被篡改，一旦监测到篡改页面，立即通过智能DNS技术阻断被篡改页面的传播，避免事态扩大。

应急对抗

- ✓ 敏感时期通过修改DNS的NS记录，把流量引到深信服安全云平台，由深信服云端安全运营专家提供7*24小时在线对抗，让互联网业务在敏感时期更加安全，更加合规放心。

SANGFOR
深信服科技

一. 深信服产品系概述

二. 云端安全产品介绍

三. 网络安全产品介绍

四. 终端系列产品介绍

五. 基础网络产品介绍

六. 数据中心产品介绍

七. 安全合规产品介绍

八. 运营管理产品介绍

九. 产品推广工具介绍

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

下一代防火墙AF

深信服AF概述

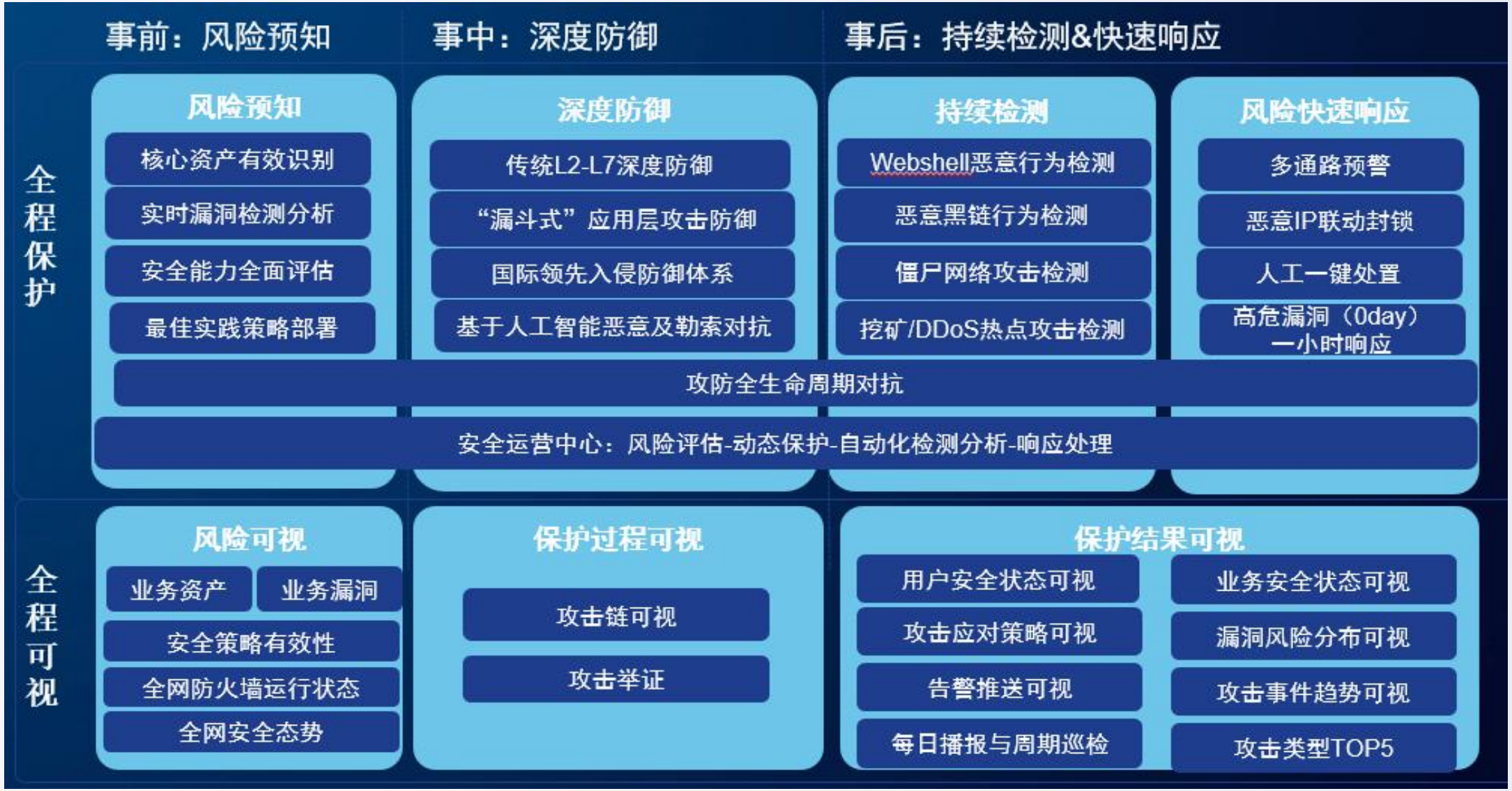
深信服下一代防火墙提出“融合安全，简单有效”价值主张，为用户业务提供全生命周期保护，真正实现全程可视和全程保护

事前	事中	事后
预知	防御	检测 / 响应
事前自动发现新增资产、评估漏洞及是否有保护策略	构建L2-7层纵深防御体系协同联动防御、关联分析	云端安全服务提供7*24小时快速响应的技术服务

- ✓ 七层防护
- ✓ 0day攻击检测
- ✓ 未知威胁检测
- ✓ APT攻击检测
- ✓ 恶意病毒检测
- ✓ WEB攻击检测
- ✓ 网络入侵检测

让安全更有效、更简单

优势点①：拥有业内最全面最实用的防火墙功能



您拥有的不仅仅是一台防火墙

优势②：提供独特的安全可视，提升全过程的安全认知能力

①对风险的认知

哪些业务要保护？	➢ 资产发现
哪里不安全？	➢ 风险识别
当前策略是否有效？	➢ 策略分析

②对保护过程的认知

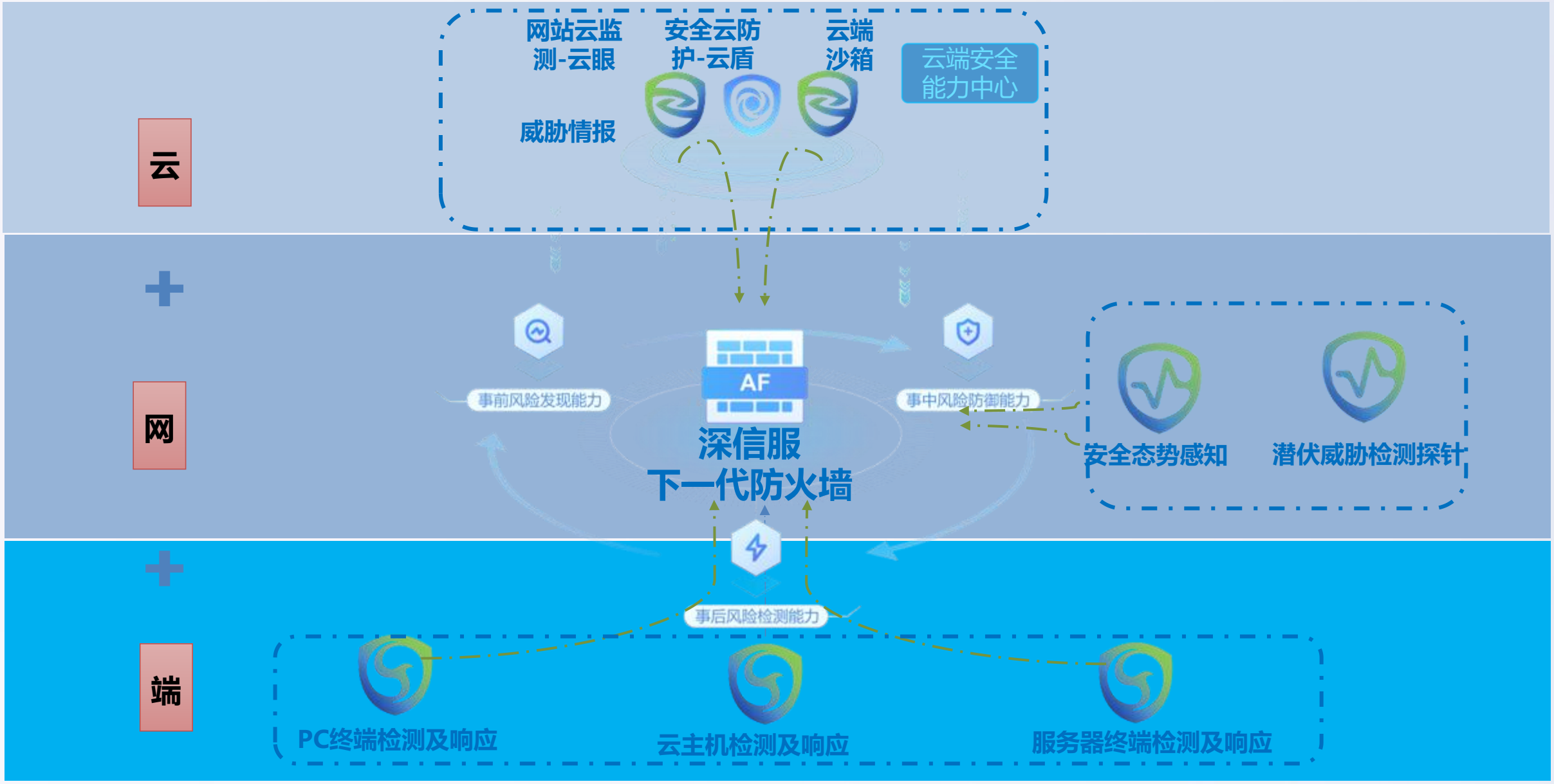
谁在攻击我？	➢ 攻击链可视
是否被绕过？	➢ 检测异常行为
是否存在误判？	➢ 攻击举证

③对保护结果的认知

安全状态怎样？	➢ 安全状态
保护的效果怎样？	➢ 安全事件
下一步做什么？	➢ 待办事项

简化安全运维 无需专业安全人员即可快速处置

优势③：强强联合 共筑云网端协同防御体系



优势④：基于AI的杀毒引擎 检测未知病毒

SANGFOR 深信服科技

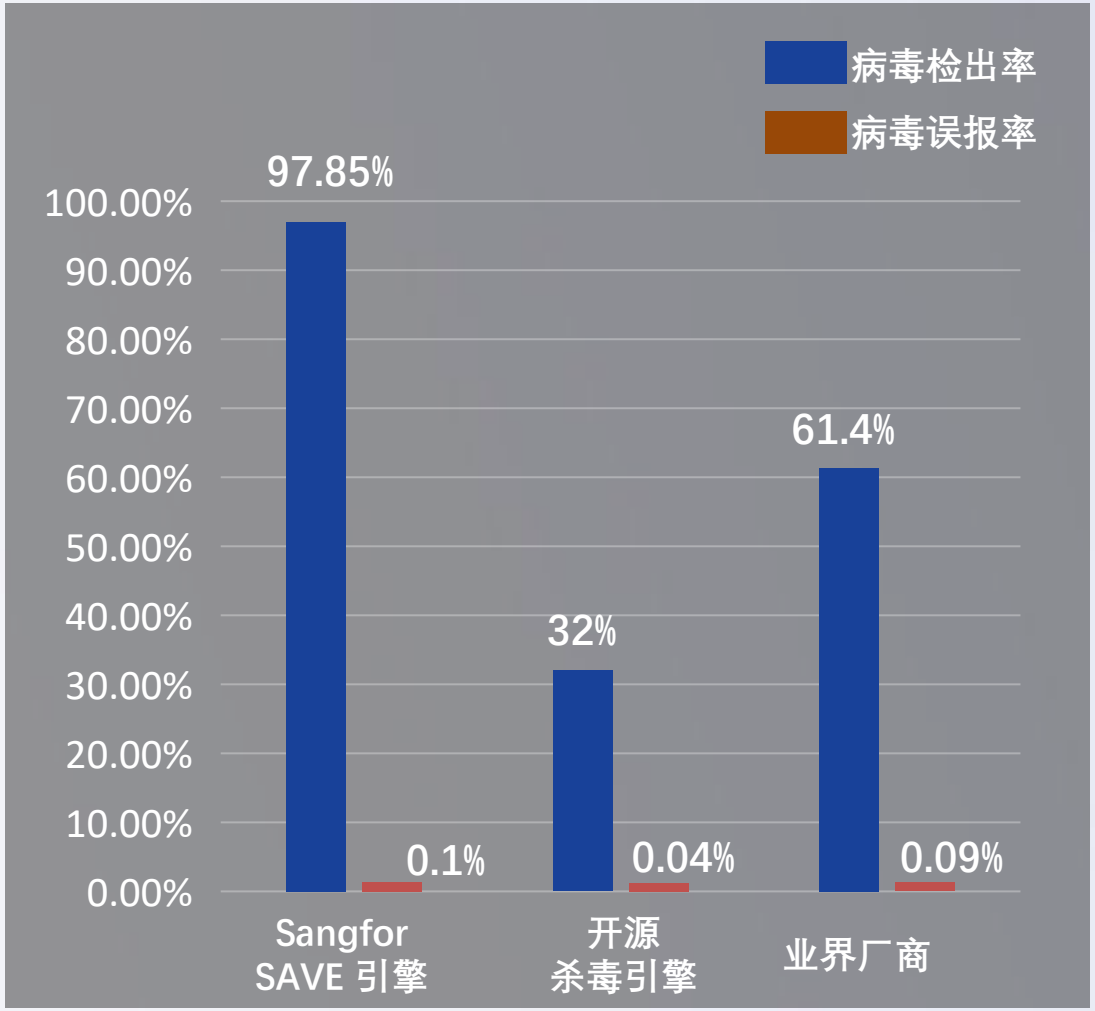
深信服人工智能杀毒引擎SAVE
Sangfor Anti-Virus Engine

创新人工智能无特征技术
准确检测未知病毒

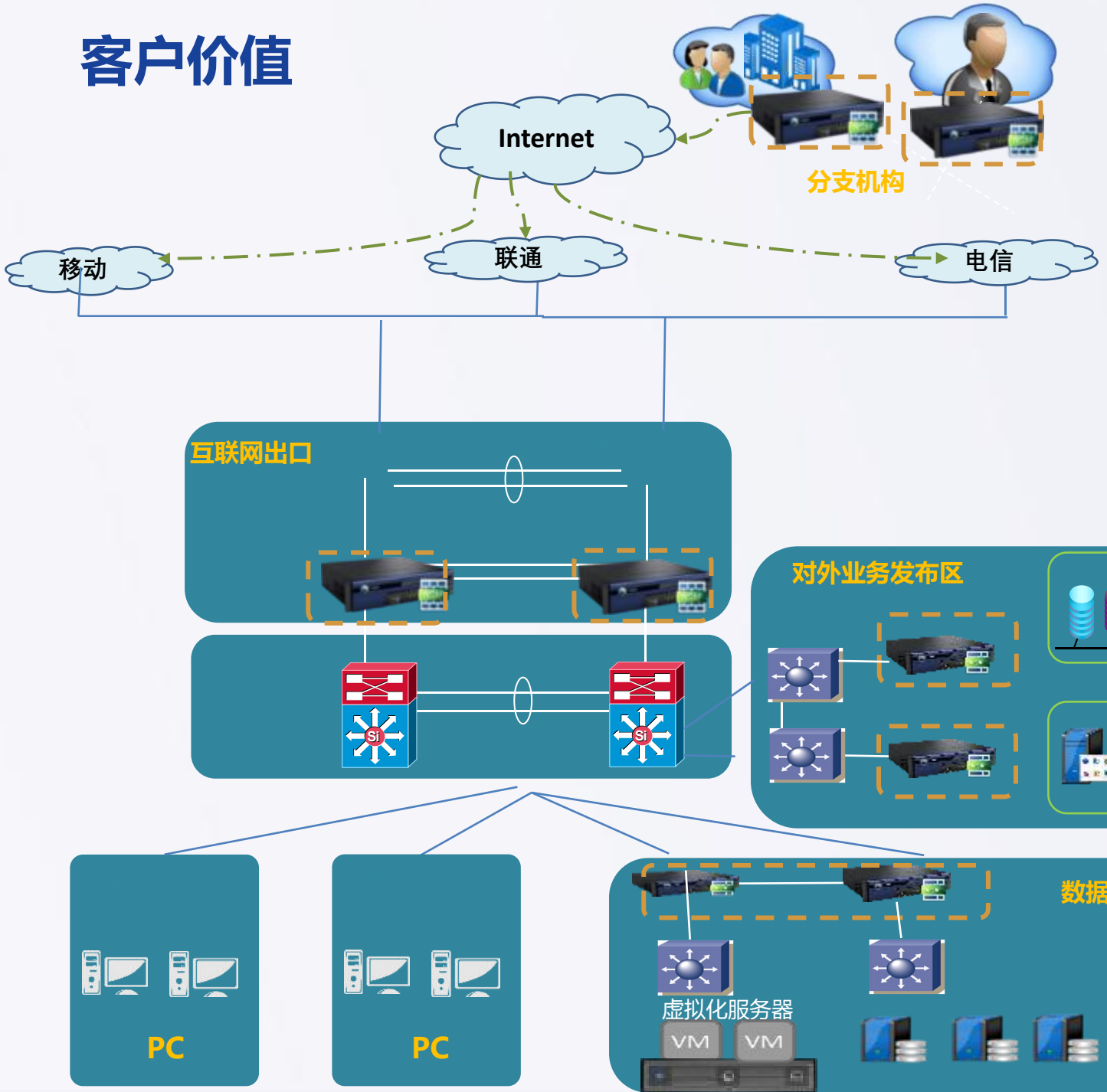
未知病毒检出率高达97.8%，对已知病毒检出率高于99%

GlobeImposter勒索病毒

查杀成功率 **100%**



客户价值



一、互联网出口及重要节点的网络访问控制
1、多链路链路出口负载均衡
2、基于应用、国家、ISP等智能选路
3、动态/双向NAT
4、基于国家、地域、时间等访问控制
5、基于应用类型、网站类型、文件类型等流量控制

二、终端上网安全管理
1、细粒度应用控制，3000+应用控制规则
2、丰富的URL类库，全面保障上网安全
3、内容安全-文件及邮件内容级深度检测

三、基于业务和用户的漏洞攻击防御
1、业务侧网络设备、服务、协议等针对业务的漏洞攻击防御，防非法入侵及绕过风险
2、用户侧防止针对用户的漏洞攻击防御，包括邮件、网页、短信等社工类攻击

四、未知威胁防御
1、通过外部情报定位未知威胁
2、云端沙箱监控恶意威胁行为，深度取证
3、海量日志关联分析，热点威胁防患于未然
4、应急响应，专杀工具，高效闭环风险

五、业务&用户为核心的全面可视化能力
1、业务及用户安全状态总览
2、事前风险全面评估、事中风险动态保护、时候持续检测，攻击链可视及溯源分析

深信服防火墙（AF）品牌实力

第一品牌，专业获得认可

- 6万+ 台在线稳定运行，广泛应用于互联网出口、对外业务发布、分支机构、数据中心等场景

持续创新，斩获多个奖项

- 公安部科学技术奖（信息系统边界防护类产品关键技术标准）
- 2018关键信息基础设施安全优秀产品之技术创新奖（2018年盘古奖）
- 2018年度中国ICT产业最佳产品奖
- 2018年度下一代防火墙技术卓越奖（2018年凌云奖）
- 下一代防火墙最具影响力奖（2018年真观奖）

典型客户案例

国家部委/省厅	应用场景	运营商用户	应用场景
国家信息中心	数据中心	中国电信集团	DMZ区
国土资源部	数据中心	中国移动四川省分公司	互联网出口
公安部	数据中心	中国联通福建省分公司	互联网出口
交通运输部	互联网出口	中国移动广东省分公司	互联网出口
外交部	互联网出口	中国联通黑龙江省分公司	互联网出口
海关总署	DMZ区	中国电信河北省分公司	互联网出口+DMZ区
工信部	数据中心	中国电信吉林省分公司	互联网出口
卫生部	数据中心	中国移动安徽省分公司	DMZ区
环保部	数据中心	中国联通江苏省分公司	互联网出口+DMZ区
农业部	DMZ区	中国联通青海省分公司	互联网出口
国资委	数据中心	中国联通湖北省分公司	互联网出口+DMZ区
国家统计局	DMZ区	中国移动陕西省分公司	互联网出口+DMZ区
最高人民法院	数据中心	中国电信云南省分公司	互联网出口+DMZ区
企业用户	**应用场景**	**金融用户**	**应用场景**
水利水电第十六工程局	互联网出口	招商银行股份有限公司	数据中心
波司登集团	广域网分支	申银万国证券股份有限公司	数据中心
国美电器集团	数据中心	兴业银行河北省分行	数据中心
东风汽车集团	互联网出口	中国保险监督管理委员会	数据中心
中国南车集团	互联网业务区	中国邮政储蓄银行浙江省分行	数据中心
中国建筑第二工程局	互联网出口	中国邮政储蓄银行安徽省分行	数据中心
中国航空国际技术有限公司	专线出口	华润深国投信托有限公司	互联网业务区
中国黄金集团	互联网业务区	华泰证券有限责任公司	互联网出口
中铁六局集团有限公司	互联网出口	光大证券股份有限公司	互联网出口
招商局集团有限公司	互联网业务区	西部证券股份有限公司	数据中心
教育用户	**应用场景**	**教育用户**	**应用场景**
北京海淀教育信息中心	互联网业务区	顺义教育信息中心	数据中心
广东教育厅	互联网业务区	福建闽侯教育局	互联网出口
上海虹口教育信息中心	互联网业务区	上海教育考试院	互联网业务区
复旦大学	互联网业务区	杭州电子科技大学	互联网出口
上海政法大学	互联网出口	华中农业大学	互联网出口
湖南农业大学	互联网出口	哈尔滨理工大学	互联网业务区

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

低端防火墙FW系列

FW系列型号发布目标

提升竞争力

- 增加末端市场的客户可覆盖度
- 增加覆盖型市场产品的竞争力

扩大渠道入口

- 通过匹配的产品，吸纳更多的覆盖型渠道加入深信服渠道体系

FW产品功能

产品价值点：安全、简单、稳定

- **网络配置智能向导**

  智能链路负载、NAT、ACL、IPSec、流量控制

- **安全策略全局配置**

  应用控制、URL、SAVE、IPS（IPS默认不开，客户可以自行勾选）

- **一体化功能序列号**

  安全功能打包为一体化功能序列号，每年10%费用

功能差别：聚焦事中防御功能与策略配置易用性，裁剪事后功能，与AF保持差异化

产品优势

SANGFOR 深信服科技

安全效果优势

对比低端市场的传统数通厂家的防火墙，在规则库的质量和数量，云端的更新能力和查杀能力都处于领先地位，深信服的安全品牌影响力也会对FW有所加持

价格优势

对比业内常见的友商，基本上FW系列的价格是友商的一半左右，对于商业市场客户是性价比非常高的选择，同时在深信服的安全品牌加持下，能够获得同价格区间产品的最高溢价能力

易用性优势

易用性优势主要体现在两个方面，一方面是上手简单，网络配置向导化、安全配置一体化，另一方面是设备支持可拓展插槽，满足客户多样化的接口需求

FW目标客户画像

销售场景：互联网出口场景、分支组网场景

目标客户画像：对于安全效果关注度不高，更关注性价比，预算有限的客户

- 商业和中小企业客户
- 区县级客户（预算有限的情况）
- 采购力每年在2W~5W左右的客户群（例如金蝶、用友的小微企业用户）
- 弱电、新建楼宇等工程类项目
- 连锁超市的多分支低预算项目
- 分销类型渠道客户群体
- ……

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

网站防护系统WAF

深信服WEB应用防火墙简介

深信服Web应用防火墙（简称WAF）专注于网站及Web应用系统的应用层安全防护，解决传统安全产品如网络防火墙、IPS、UTM等安全产品难以应对应用层深度防御的问题，有效防御网站及Web应用系统面临如0WASP TOP 10中定义的常见威胁，并·且可以快速应对非法攻击者针对Web业务发起的0Day威胁、未知威胁等攻击，实现 用户Web 业务应用安全与可靠交付。

- 降低用户数据泄漏风险
- 避免组织声誉影响
- 优化WEB业务访问体验

产品核心功能

防止网站非法入侵

- Web漏洞攻击防护
- Web通用攻击防护
- SAVE杀毒引擎
- 云端沙盒检测
- 联动云脑规则实时下发

严格的访问控制策略

- 基于IP和Session的访问控制策略
- 暴力破解攻击识别与拦截
- 网站弱口令识别与拦截

防止敏感数据非法获取

- Webshell防护
- 敏感信息过滤
- 失陷主机检测
- 非法下载限制

优化WEB业务访问体验

- 应用加速
- SSL卸载
- 恶意注册行为识别与拦截

避免组织声誉影响

- 网页防篡改
- 防恶意扫描
- 黑链检测
- 联动云眼持续监测

产品优势

文件过滤驱动技术

- ✓ 支持静态页面和动态页面防篡改，减少系统资源消耗，实现主动防御

监测防御响应闭环

- ✓ 7*24小时告警监测
- ✓ AI 安全专家自动化分析
- ✓ 云端大数据识别高级威胁
- ✓ 多方安全威胁情报共享

正则匹配与语法分析结合

- ✓ 基于特征签名机制，深信服WAF采用Sangfor Regex正则引擎，快速识别已知威胁;
- ✓ 基于威胁攻击利用漏洞原理，深信服WAF建立攻击判定模型，快速识别攻击变种，降低漏报和误报

融入SAVE实现服务器病毒防护

- ✓ 算法主动优化
- ✓ 样本自动收集和预测

品牌认可度

2014年深信服Web应用防火墙通过NSS Labs测试，并获得最高级别“Recommended”推荐级，深信服成为国内首家获得Web应用防护“Recommended”推荐级的安全厂商。

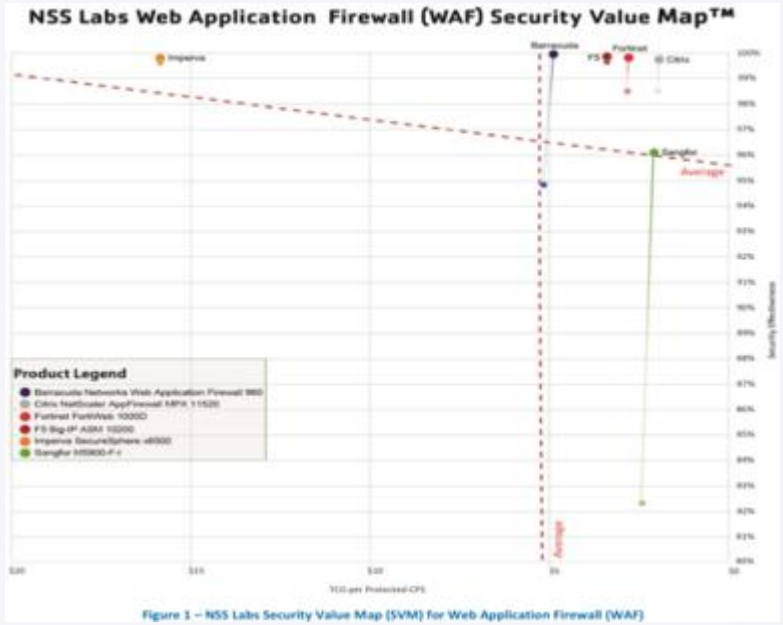


Figure 1 – NSS Labs Security Value Map (SVM) for Web Application Firewall (WAF)

NSS LABS RECOMMENDED

深信服WAF成功入围多个集中采购平台

中央政府采购网 www.zycg.gov.cn

中央政府采购目录

税务采购网 CTAXCCGP.ZCY.GOV.CN

国家税务总局目录

中国移动通信 CHINA MOBILE

中国移动集采目录

中国电信 CHINA TELECOM

中国电信集采目录

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

入侵防御系统IPS

产品概述

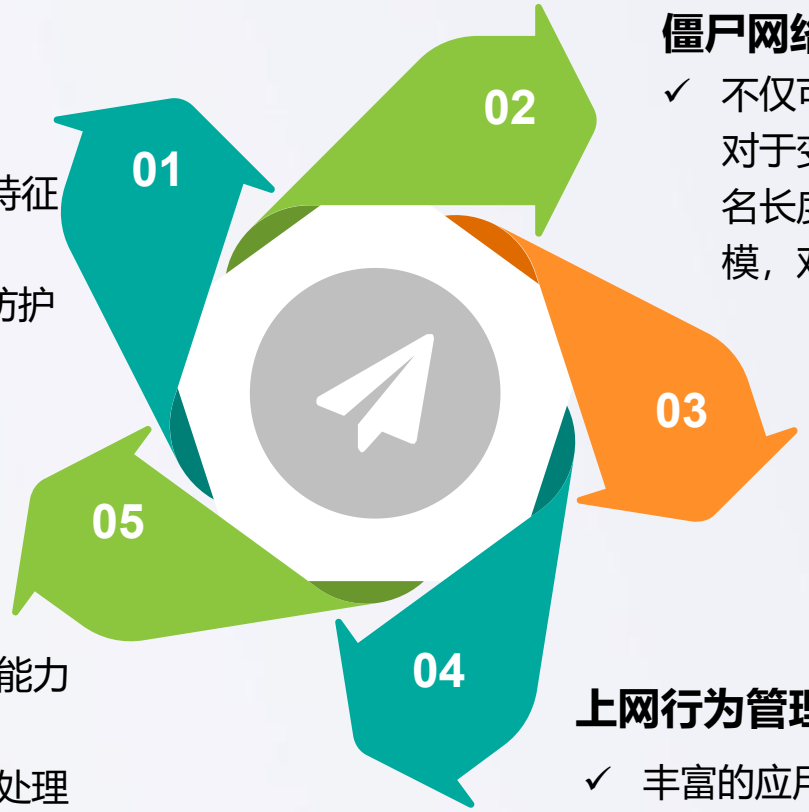
深信服下一代入侵防御系统围绕“全面、精准、快速、简单”的核心理念，通过对网络流量的深度解析，可及时准确发现各类非法入侵攻击行为，并执行实时精确阻断。深信服入侵防御系统不仅可以应对对漏洞攻击，而且更加强调通过多维度的检测技术包含基于AI和沙箱等实现识别新型威胁和未知威胁检测的全面和精确性，同时借助云端能力实现特征和情报快速更新，提供了完整的立体式入侵防御架构

- 已知和未知漏洞攻击全面防护
- 新型高危攻击即时防护
- 有效降低漏报误报
- 轻松管理，降低运维成本

核心功能

漏洞攻击防护功能

- ✓ 优化的Snort检测引擎
- ✓ 已知漏洞攻击防护（7000+漏洞特征库）
- ✓ 基于白流量建模的未知漏洞攻击防护



僵尸网络检测

- ✓ 不仅可以基于情报检测僵尸网络，对于变形的僵尸网络，可以对域名长度、域名杂乱程度等维度建模，对偏离的离散点精准定位

病毒攻击防护

- ✓ 通过MD5库检测已知病毒，同时基于SAVE安全智能检测引擎、云端威胁情报和云沙箱，能够有效防御变种勒索病毒和其他未知病毒的攻击

丰富的联动功能

- ✓ 联动云脑快速更新安全能力
- ✓ 联动云守智能运营
- ✓ 联动EDR安全问题闭环处理

上网行为管理

- ✓ 丰富的应用特征识别库
- ✓ IM与P2P控制
- ✓ 业界领先URL过滤功能
- ✓ 股票软件和网络游戏
- ✓ 网页及邮件内容过滤

产品优势

建立白流量模型，定位偏离模型的未知恶意流量

未知恶意流量防护

海量多维度威胁情报下发与实时云端检测技术，快速更新安全能力，热门威胁特征10分钟下发，热点事件1小时响应

僵尸网络智能检测

联动云脑快速更新

勒索病毒有效防护

不仅可以基于情报检测僵尸网络，对于变形僵尸网络，可以对域名长度、域名杂乱程度等维度建模，对偏离的离散点精准定位

通过SAVE安全智能检测引擎、云端威胁情报和云沙箱，能够有效防御变种勒索病毒和其他未知威胁的攻击

人工智能 → 深度学习 → 优化算法

收集 → 学习样本 → 预测样本 → 自动防御

客户价值

安全专家

威胁情报

云端检测引擎

全面保护

- ✓ 7000+已知漏洞攻击检测与防御
- ✓ 过白流量建模，检测未知漏洞攻击
- ✓ 联动EDR实现网端全面保护
- ✓ 基于URL的全面行为管理

精准检测

- ✓ 多维度的智能检测技术（如save、NTA和云沙箱）全面检测恶意文件、僵尸网络和未知威胁
- ✓ 建立用户业务特征模型，解决代码不规范导致的误判
- ✓ 通过云守功能，个性化安全策略定制降低误判

快速更新

- ✓ 优化检测引擎，根据协议/端口等对规则进行分类，提高匹配速度和效率；
- ✓ 热门威胁特征10分钟下发，全球热点事件1小时响应
- ✓ 安全规则实时更新

简单运维

- ✓ 安全运营中心助力可视化管理
- ✓ 安全报表简单易懂
- ✓ “一键式”“向导式”简化运维

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

上网行为管理AC

深信服AC概述

2005年，深信服科技推出中国第一款专业上网行为管理产品，截至到2018年底，该产品的用户数量已达30000多家，其中超过8000家为中高端客户，因其优异的表现，连续十年市场占有率第一，也是国内唯一 一家入选Gartner SWG魔力象限厂商。

用户认证

丰富的认证方式
有线、无线统一认证

应用封堵

精细的应用识别、管控(网页过滤和应用控制)

流量管控

合理分配带宽
保证核心业务运行

行为审计

全面的上网行为审计
规避违法和泄密风险

产品优势

①全面准确识别常用应用和网站

- 2800+种应用（几乎所有常见应用）
- 1000+种移动应用
- 老旧应用及时淘汰
- 千万级URL分类库
- 每2周更新一次，已持续12年
- 支持IM聊天内容审计
- 支持微信和QQ的聊天内容、发文件等审计
- 支持APP审计/移动应用审计：包括账号审计、内容审计（非加密类应用）、应用行为审计

②支持SSL加密内容识别技术

- 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。

产品优势

③有线/无线统一上网行为管理

- 有线无线统一管理界面
- 用户内部联动，简化运维
- 二维码、短信、微信等多种认证方式

④按需审计和敏感保护

- 可针对部分人员免审计
- 可对管理员授权持有审计key

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。

客户价值

提高工作效率

通过应用控制，限制与工作无关的上网行为

规避违法风险

记录审计用户上网行为，避免肆意外发非法言论

提高带宽利用率

合理分配带宽，动态调节，减少浪费，提高带宽应用价值

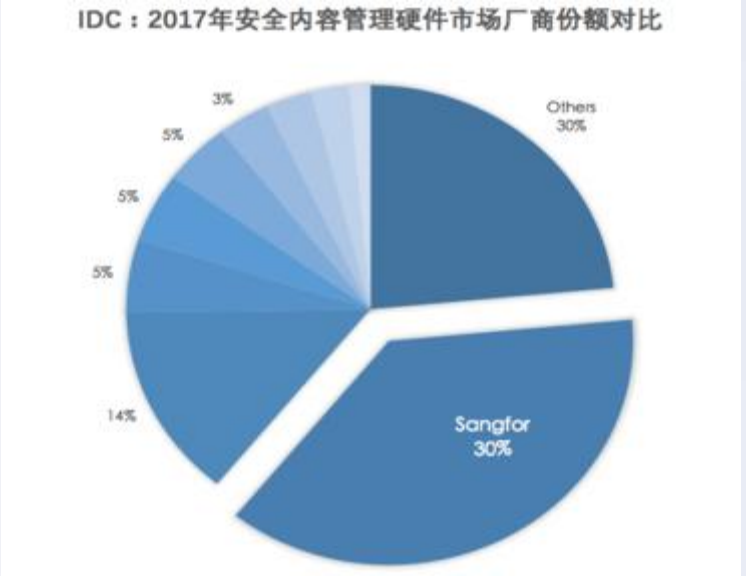
安全保障

拦截不良网页，提供安全接入
提高内网安全性

深信服上网行为管理（AC）品牌实力

市场第一 连续10年中国市场第一

- 2017年市场占有率30%，**超第2和第3名的总和**；
- **中国唯一入围**国际Gartner SWG魔力象限的产品，并且**连续6年**成功入围；



技术第一　拥有国内最为领先的技术

- 创新推出上网行为感知系统；
- 拥有全国最完善的应用识别特征库和URL库；
- 获得17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最高等级认证；
- 率先获得IPv6 Ready认证的上网行为管理产品；


资质认定
授权证书
证书编号：（2017）国认监认字（619）号
名称：国家网络与信息系统安全产品质量监督检验中心
地址：上海市岳阳路76号（200031）
经审查，你机构已具备国家有关法律、行政法规规定的基本条件和能力，现予批准，可以向社会出具具有证明作用的数据和结果，特发此证。
检测能力见证书附表。
准许使用徽标

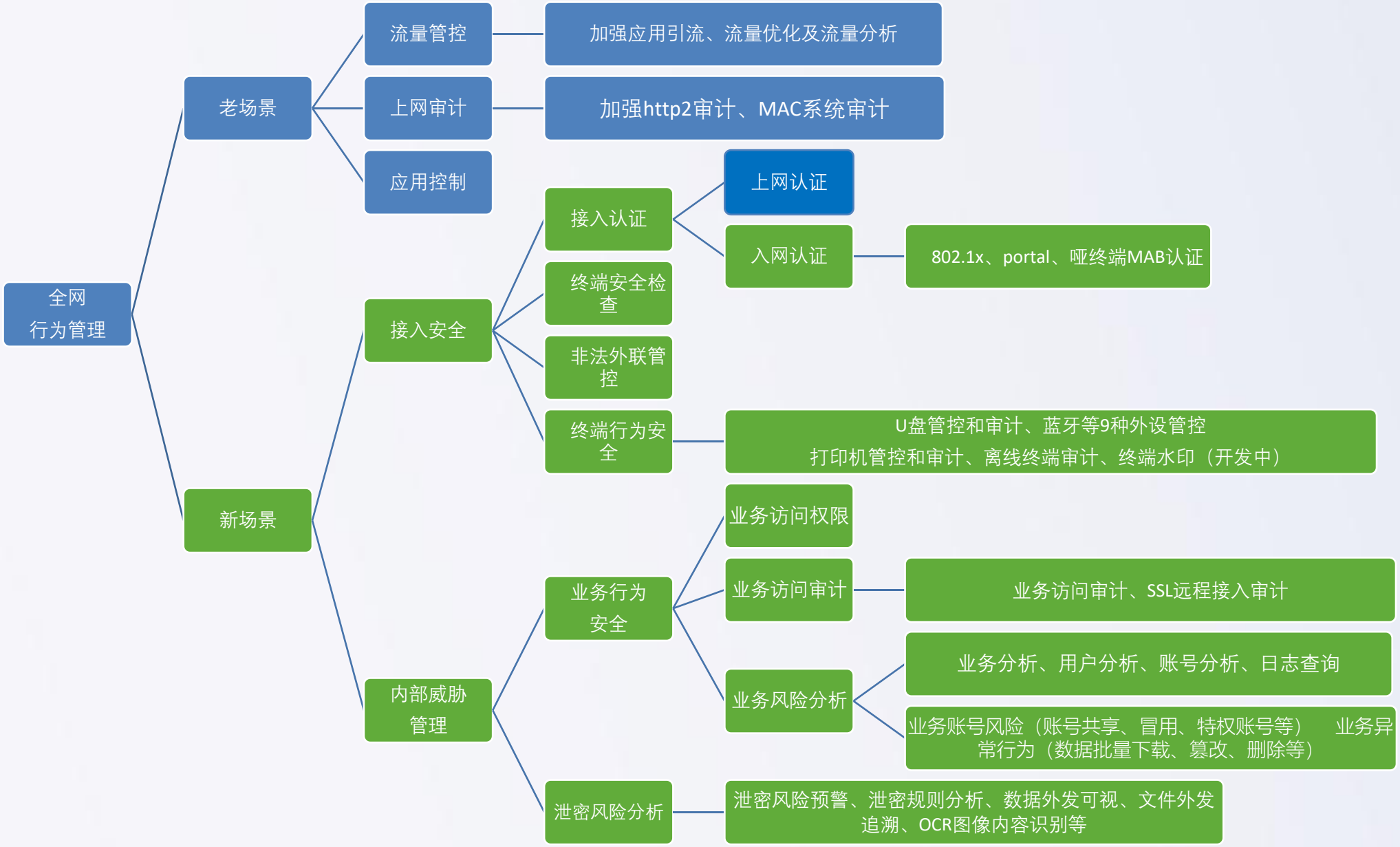
客户第一　拥有国内最为领先的技术

- **40000多家**全国各行业用户；
- **80%** 进入世界500强的中国企业；
- **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（中农建工交五大行，招商、兴业、民生等12家股份制银行）；
- 服务于**世界互联网大会、奥运会、世博会、亚运会、青奥会**等大型活动；

典型客户案例

政府	金融	教育科研	企业集团	运营商及能源
国家天文台信息中心	招商银行	中国人民大学	南方航空公司	中国移动广东分公司
国务院参事室	中国进出口银行总行	中国政法大学	中兴通讯股份有限公司	中国联通陕西分公司
国务院新闻办公室	安邦财产保险股份有限公司	中央广播电视大学	南光集团	中国石油天然气股份有限公司
安徽省财政厅	中国人寿保险股份有限公司	华南师范大学	青岛啤酒	中国石化湖南分公司
湖南省农业厅	浦发银行	北京航空航天大学	华润万家	中国石化天津分公司
河北省审计厅	中信银行	杭州电子科技大学	吉利汽车	中国石油东北销售分公司
云南省交通厅	安信证券	厦门教育局	上海文广传媒集团	中国石油安徽销售分公司
江西省文化厅	华夏基金管理有限公司	北京朝阳区教育局	三生集团	中核集团泰山核电有限公司

上网行为管理—>全网行为管理

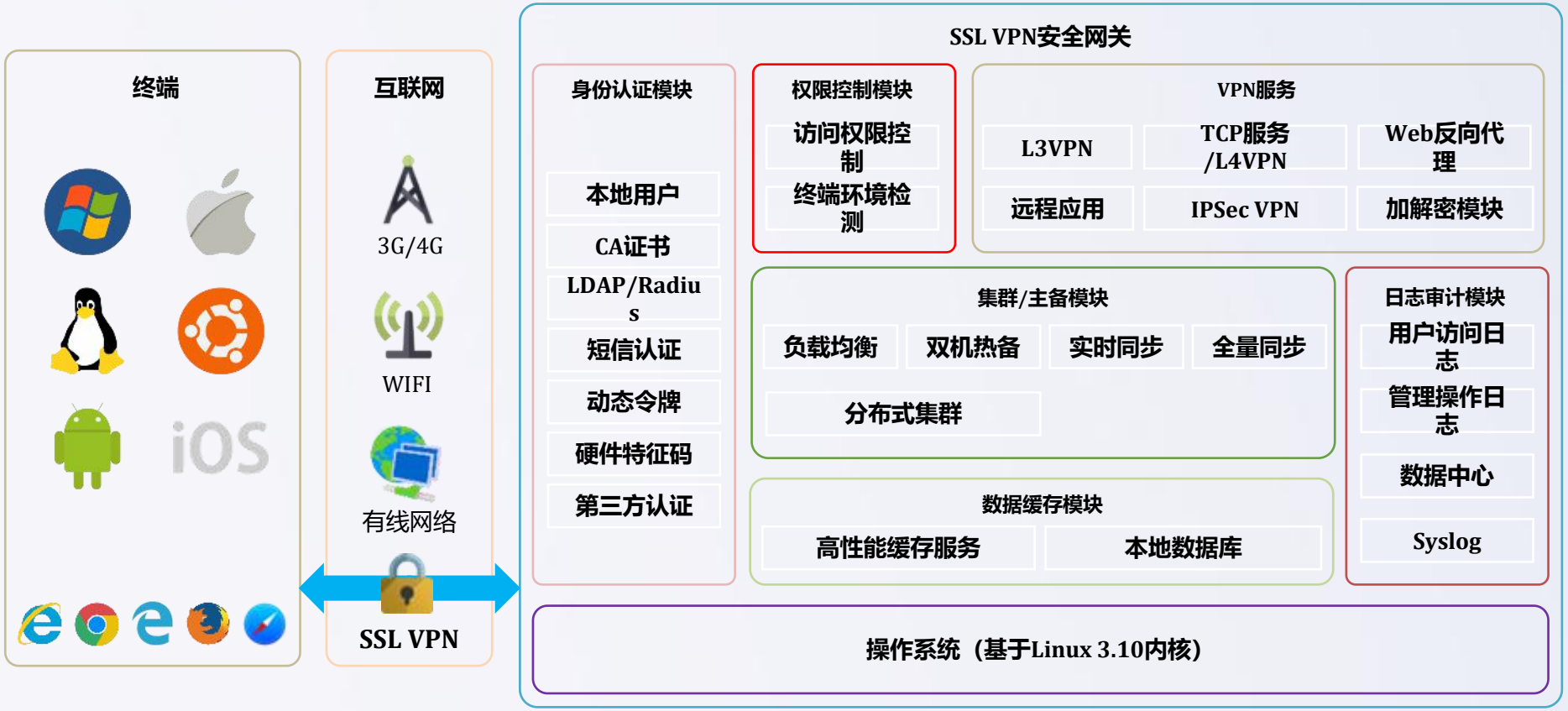


SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

SSL VPN

SSL VPN产品概述

深信服VPN是一款面向链路通信安全的技术产品， 自入市以来，深信服科技持续引领着业界内的技术创新，于2005年推出全球第一款IPsec/SSL二合一的产品，从2008年开始，便以超过三分之一的市场，一直占据VPN中国市场第一的位置



技术优势①：端到端保护 全兼容

端到端保护
——保障系统接入安全

全兼容
——保障用户使用体验

技术优势②：丰富灵活的认证方式

多种认证方式、完善的认证体系

- 使得企业在选择的时候，可以根据相应的安全级别，对客户端的认证方式进行组合，最大限度地保证了接入用户的合法性和企业内网资源的高度安全。

内置的CA中心提供完整认证体系

- SANGFOR SSL VPN安全网关内置了CA中心，企业或者事业单位可自建CA中心，用户可不必购买单独的CA认证体系，为企业减少了投入成本。同时，SANGFOR SSL VPN安全网关也可无缝支持已有的第三方CA认证。

客户价值

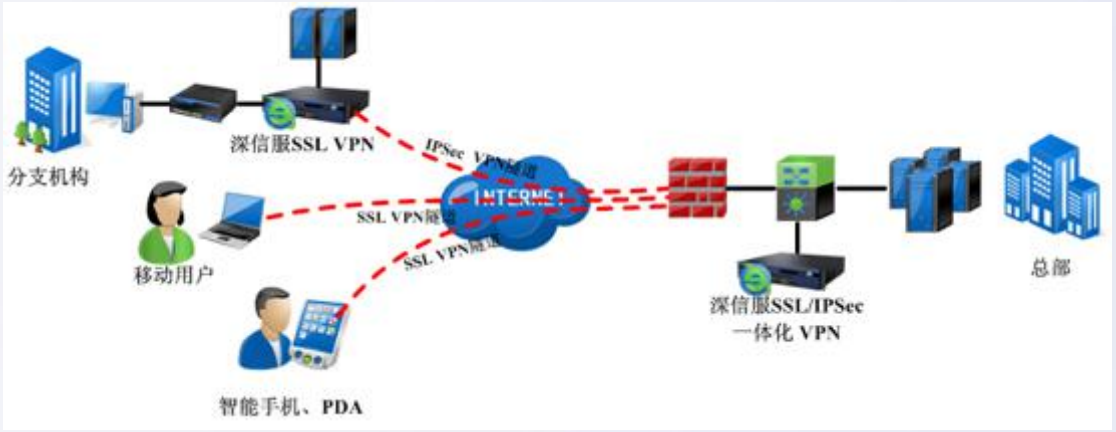
组网

A 分支组网

- 核心业务系统安全加固（大专网建设小专网）
- Web VPN （教育行业应用较多）
- 移动办公接入，随时随地接入单位业务系统办公

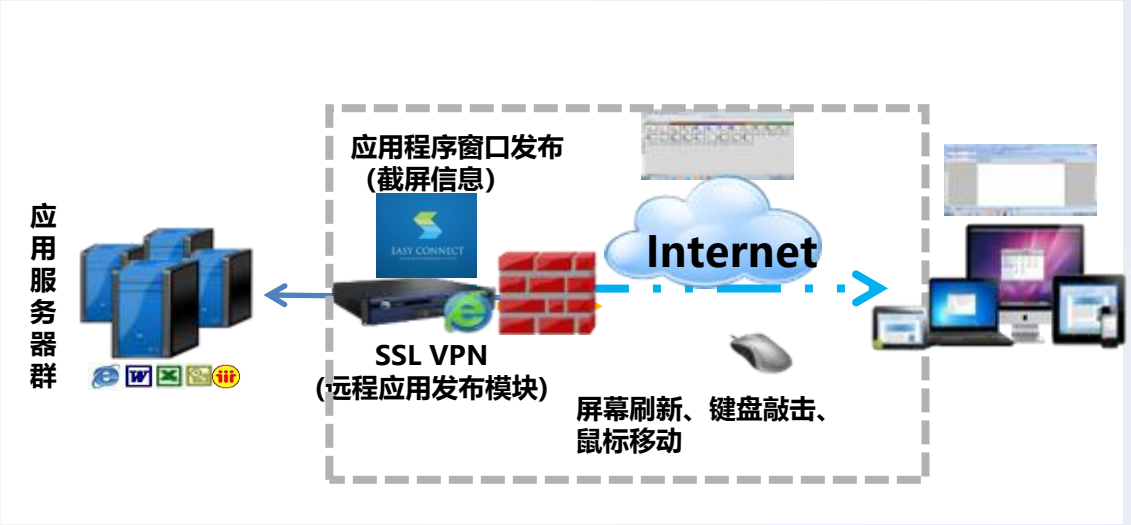
B 总部组网

- 替换专线
- 专线备份



远程应用发布

- 应用加速
- 数据防泄密
- 解决兼容性问题

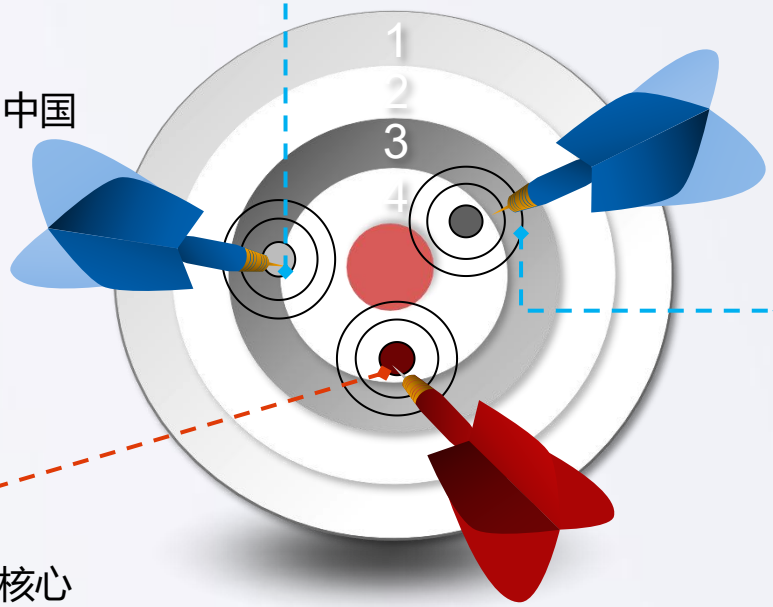


支持合规改造：关键信息基础设施行业对应的VPN产品需要支持国家商用密码算法，否则要通过国密产品的进行原设备的升级替换

品牌实力

市场第一

- ✓ 国内唯一入围 Gartner魔力象限
- ✓ 连续九年市场占有率第一
- ✓ 入围中央政府采购、国税总局、中国工商银行总行集采目录



技术第一

- ✓ 国家SSL/IPSEC VPN技术标准核心制定者
- ✓ 2005年推出创新推出SSL、IPSEC一体化的VPN 安全网关
- ✓ 最强的兼容性，保障用户使用体验

高端用户第一

- ✓ 拥有业内最多的高端客户，包括国务院国资委、海关总署、环保部、公安部、最高检、最高法、中国移动、中国联通、中国人民银行、银监会、伊利集团、海尔集团、三一重工、中广核等中国500 强企业中，有70%的企业选择了深信服SSL VPN 产品

客户案例

税务	财政	公检法	卫生环保	政府
国家税务总局	湖南省财政厅	中华人民共和国最高人民检察院	卫生部卫生监督中心	四川省工商局
云南省国家税务局	北京市财政厅	公安部边防管理局	安徽省卫生厅	山西省信访局
山东省国家税务局	乐山市中山财政局	公安部安保局	西安市卫生局	厦门市劳保局
福建省地方税务局	中华人民共和国财政部	安徽省公安厅	山西省卫生厅	青岛人社局
河北省地方税务局	云南省财政厅	福建省公安厅	湖南省卫生厅	广西省社保局
海南省地方税务局	辽宁省财政厅	广东省公安厅	贵州省卫生厅	济南人社局
重庆市地方税务局	西藏自治区财政厅	广西壮族自治区公安厅	云南省卫生厅	浙江省气象局
南京市地方税务局	宁夏回族自治区财政厅	海南省公安厅交警总队	江西省卫生厅	玉林市政府
广州市地方税务局	广西壮族自治区财政厅	河南省公安厅国保局	湖北省卫生厅	包头市政府
深圳市地方税务局	四川省财政厅	黑龙江省公安厅	青海省卫生厅	上海市宝山区政府
合肥市地方税务局	湖北省财政厅	湖北省公安厅国保局	浙江省卫生厅	上海市交易管理局
四川省国家税务局	青海省财政厅	江西省公安厅国保总队	广东省卫生厅	长沙市开福区政府
乐山市地方税务局	黑龙江省财政厅	辽宁省公安厅	山东省卫生厅	**教育**
西藏自治区国家税务局	广东省财政厅票据监管	内蒙古公安厅	山东省环保厅	浙江大学
辽宁省国家税务局	厦门市财政局	青海省公安厅	江苏省环保厅	中国政法大学
贵州省国家税务局	石家庄市财政局	山东省公安厅	云南省环保厅	广西师范大学
青海省国家税务局	沈阳市财政局	山西省公安厅禁毒局	浙江省环保厅	河北农业大学
广东省国家税务局	兰州市财政局	陕西省公安厅	辽宁省环保厅	中国青少年研究中心
河北省国家税务局	合肥市财政局	陕西省公安厅交通管理局	安徽省环保厅	中国人民大学
江苏省国家税务局	武汉市财政局	新疆自治区公安厅	江西省环保厅	浙江省教育厅
深圳市国家税务局	晋城市财政局	北京市人民检察院	福建省环保厅	同济大学
郑州市国家税务局	钦州财政局	南宁市人民检察院	宁夏自治区环保厅	电子科技大学
云南省地方税务局	新疆维吾尔自治区财政厅	甘肃省公安厅交警总队车管所	河北省卫生厅	河北省水利厅

客户案例

航空企业	汽车企业	央企	金融
济南国际机场股份有限公司	东风汽车有限公司	中国航天科技集团	兴业银行
中国货运航空有限公司	天津一汽夏利	中国远洋运输集团	东莞银行
中远国际航空货运代理有限公司	南京菲亚特集团	中南集团	中国人寿
中航工业商用发动机有限公司	上汽通用五菱汽车公司	中国航空工业集团公司	中国人民银行
上海国际机场股份有限公司	东风汽车有限公司	中国长江三峡集团公司	中国工商银行
上海机场（集团）有限公司	比亚迪股份有限公司	中国电子信息产业集团有限公司	中国农业银行
青岛机场	永康众泰汽车有限公司	中国铝业公司	中国农业银行上海分行
西部机场集团	东风雷诺汽车有限公司	中粮集团有限公司	招商银行
昆明航空有限公司	东风本田汽车有限公司	中国五矿集团公司	中信银行
深圳航空有限公司	东风汽车股份有限公司	中国通用技术控股有限责任公司	邮储银行
萧山机场	厦门金龙联合汽车工业有限公司	中国储备粮管理总公司	中国银监会
浙江长龙航空有限公司	长城汽车集团有限公司	华润（集团）有限公司	财富证券
顺丰航空有限公司	东风小康汽车有限公司	中国商用飞机有限责任公司	华林证券
民航凯亚新疆分公司	吉林金洪汽车部件股份有限公司	中国节能环保集团公司	西南证券
中国航油新疆分公司	中国润东汽车集团有限公司	中国国际工程咨询公司	东兴证券
航天通信股份集团有限公司	广汽丰田汽车有限公司	中国华孚贸易发展集团公司	宏源证券
瑞丽航空有限公司	京津冀城际铁路投资有限公司	中国诚通控股集团有限公司	中信证券
武汉天河机场集团	中国重汽集团	中国煤炭科工集团有限公司	一德证券
上海虹桥机场股份有限公司	长安汽车责任有限公司	中国中钢集团公司	中银基金
云南红土航空股份有限公司	东风康明斯发动机有限公司	中国工艺（集团）公司	中银保险
上海飞机制造厂有限公司	林德英利（天津）汽车部件有限公司	中国恒天集团有限公司	长安责任保险
香港航空	长春英利汽车工业股份有限公司	中国机械工业集团有限公司	中国建设银行吉林分行

SANGFOR 深信服科技

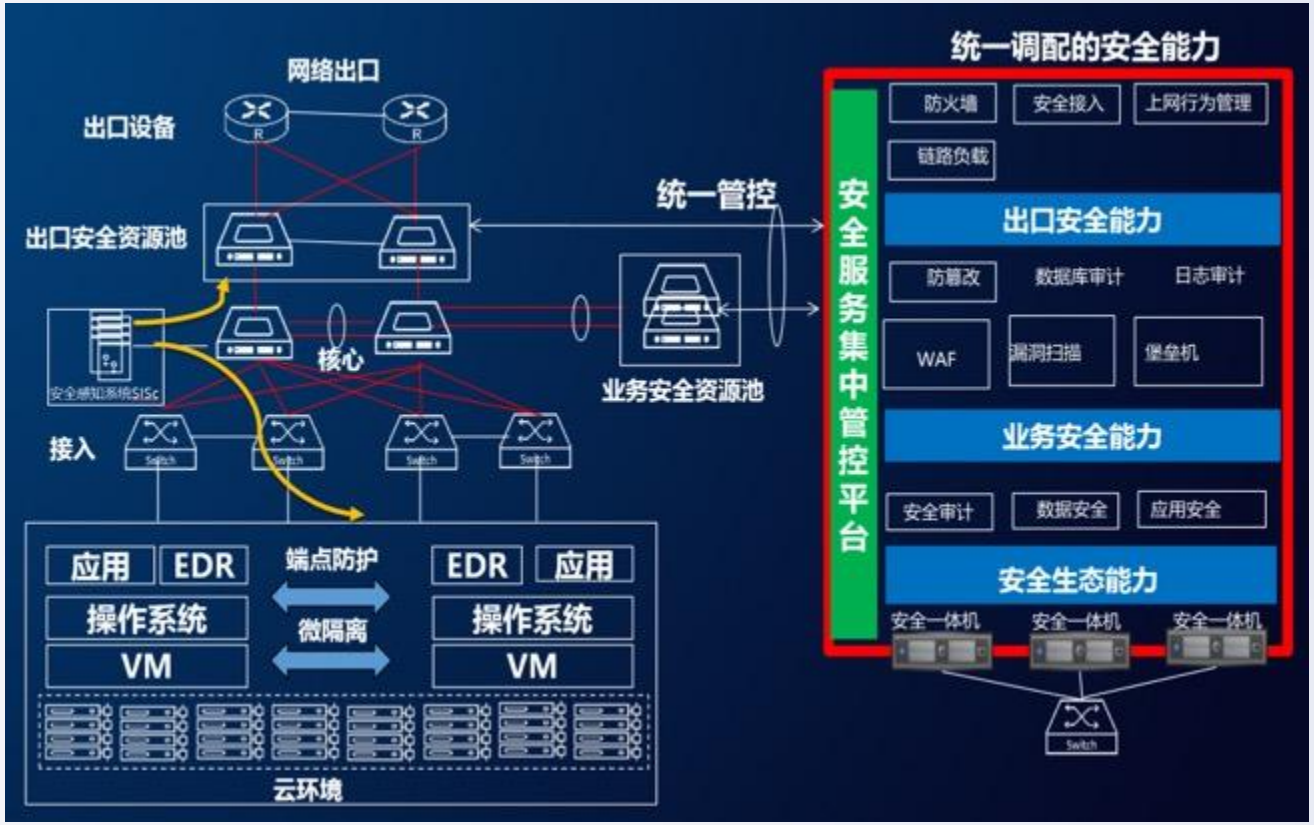
深信服智安全 SANGFOR SECURITY

云安全资源池平台

产品概述

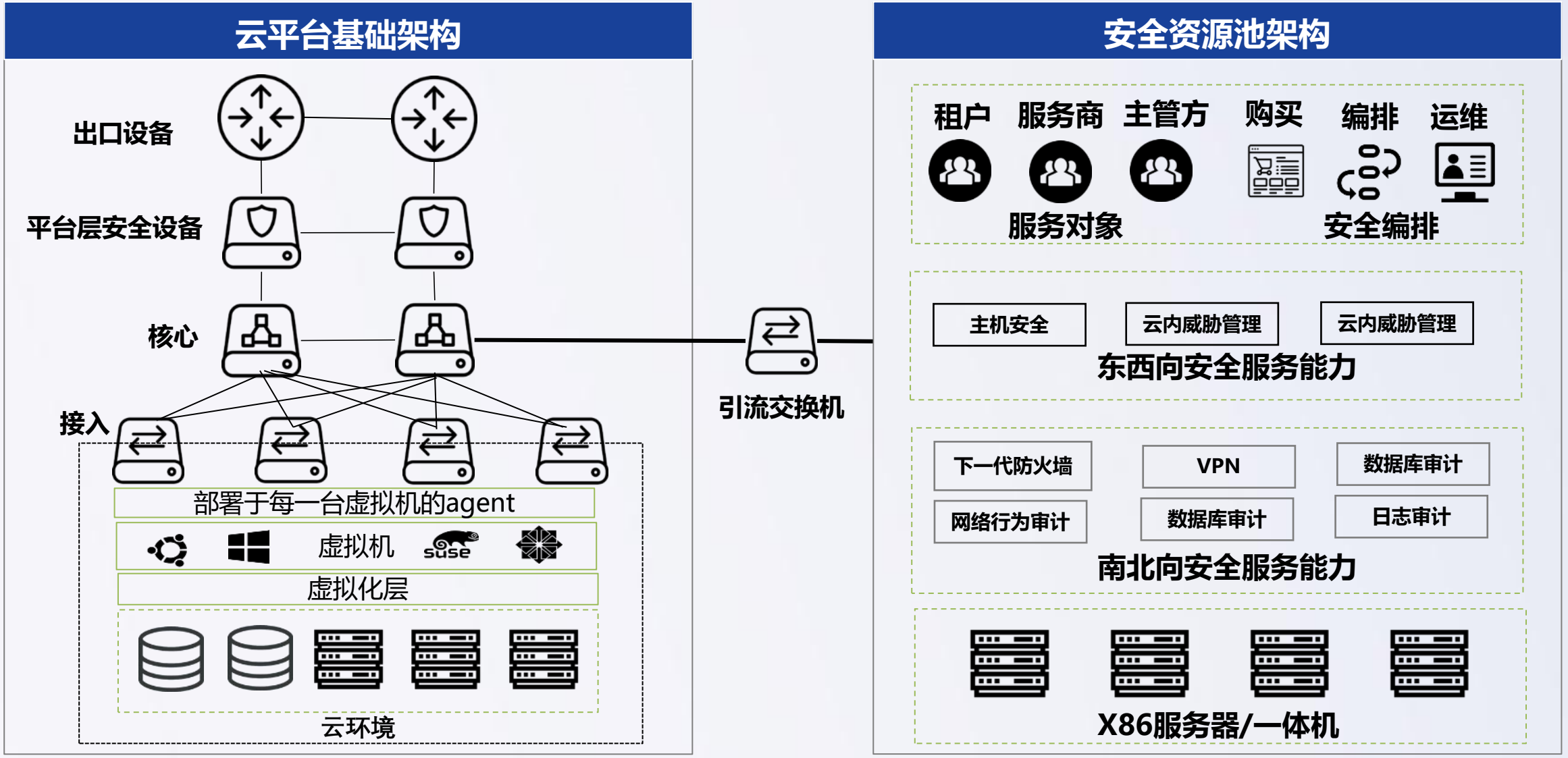
基于软件定义安全技术的安全能力交付平台

- 深信服安全资源池系统，通过以安全组件的形式向用户提供丰富的安全监测和防护能力，安全资源池与云平台解耦，广泛应用于新建、已建、扩建的云场景及传统数据数据中心安全建设场景。在安全资源池平台中，可将深信服下一代防火墙、上网行为管理、SSL VPN、数据库审计及应用交付等各类硬件设备以软件形式提供。
- 深信服安全资源池支持整合第三方生态安全组件，例如堡垒机、日志审计及配置核查等各类安全能力。
- 深信服安全资源池方案目前已帮助全国各类省市级政务云的安全建设，也帮助客户完成了大量交通云、警务云、IDC数据中心及各类数据中心的安全建设。



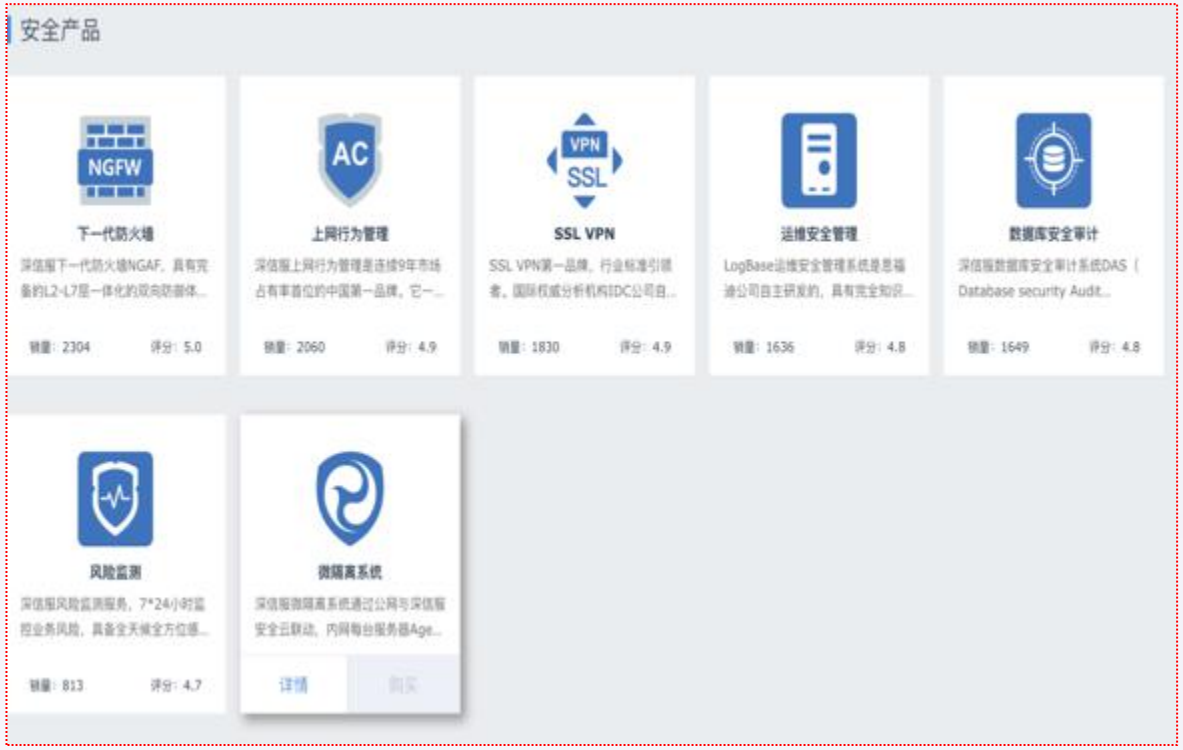
整体架构

只需通过标准X86服务器搭配上安全资源池系统，就可以向租户提供丰富的安全服务。安全资源池与云平台解耦、旁挂部署，通过配置策略路由进行租户VPC网络打通，广泛适用于新建、扩建、已建的政务云场景



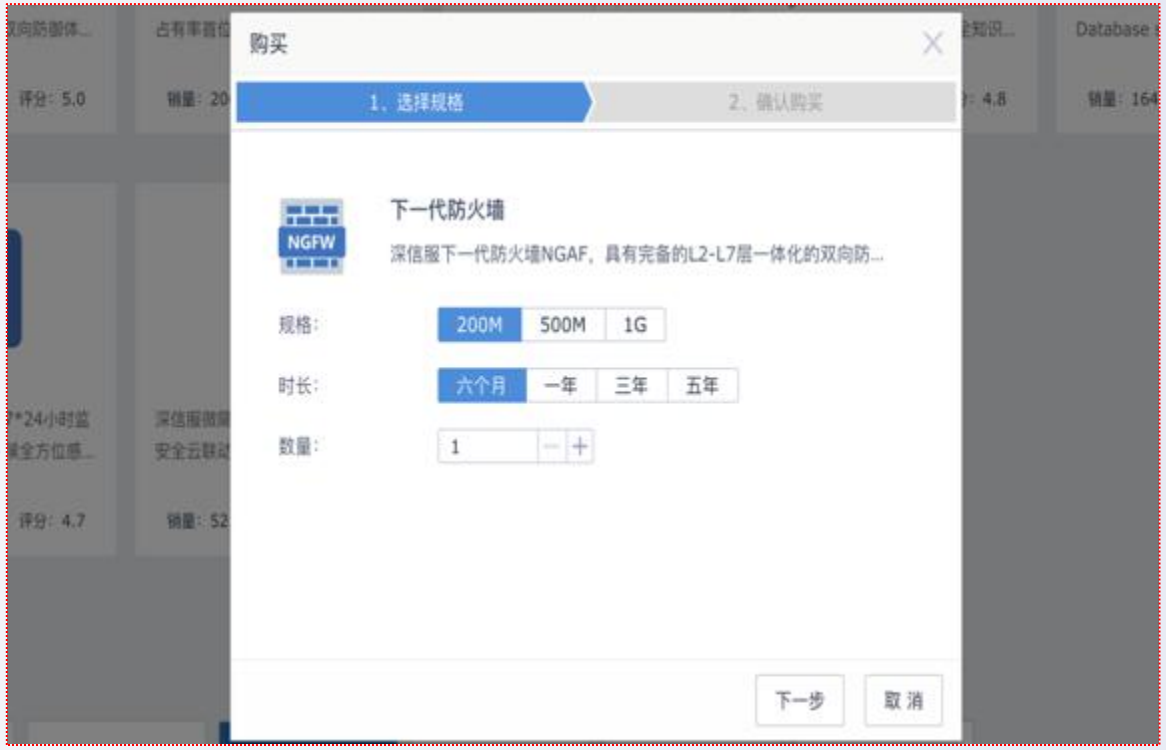
功能特性

能力丰富，助力合规



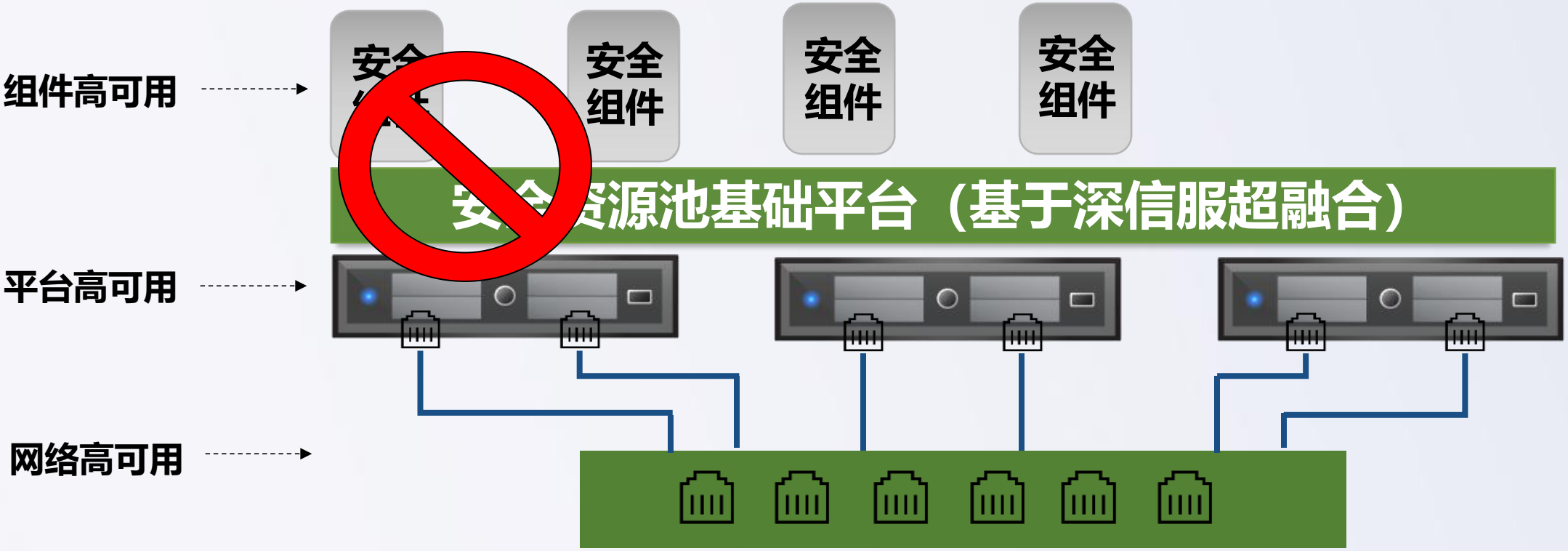
深信服安全资源池，可向租户提供从安全接入到整体安全运营的全业务生命周期安全组件，传统安全建设通过买安全产品来满足合规需求，现在都通过安全资源池的组件交付依然能够满足。

安全能力按需使用，弹性扩展

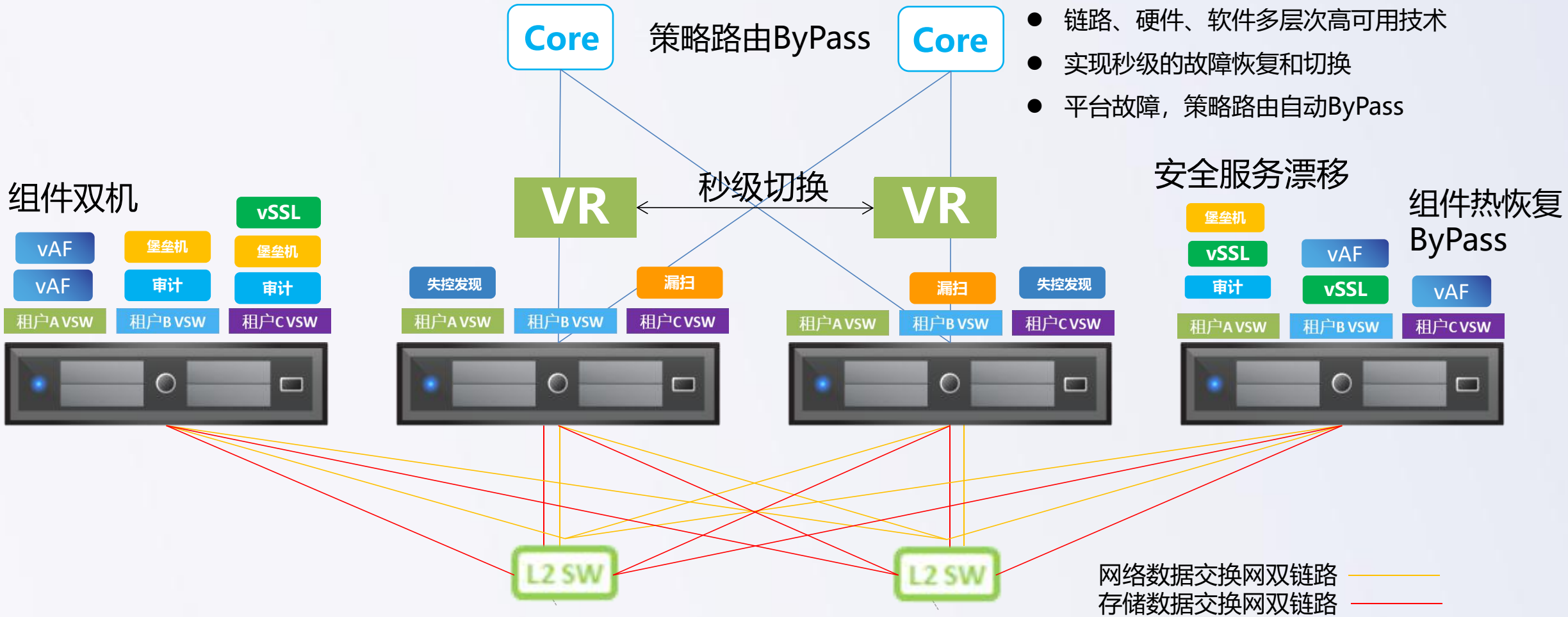


云平台租户通过简单的自助服务申请、开通流程即可快速获得对应的安全服务。云运营方可以像交付计算、存储资源一样进行安全服务资源交付，符合国家对云资源服务的采购要求。

产品优势①：高可用性



多层次的高可用设计


Core
策略路由ByPass
Core
链路、硬件、软件多层次高可用技术
实现秒级的故障恢复和切换
平台故障，策略路由自动ByPass
组件双机
秒级切换
安全服务漂移
组件热恢复
ByPass
VR
VR
vSSL
vAF
堡垒机
堡垒机
vAF
审计
审计
租户A VSW
租户B VSW
租户C VSW
失控发现
漏扫
租户A VSW
租户B VSW
租户C VSW
漏扫
失控发现
租户A VSW
租户B VSW
租户C VSW
堡垒机
vSSL
vAF
审计
vSSL
vAF
租户A VSW
租户B VSW
租户C VSW
L2 SW
L2 SW
网络数据交换网双链路
存储数据交换网双链路

产品优势②：平台性能可线性扩充

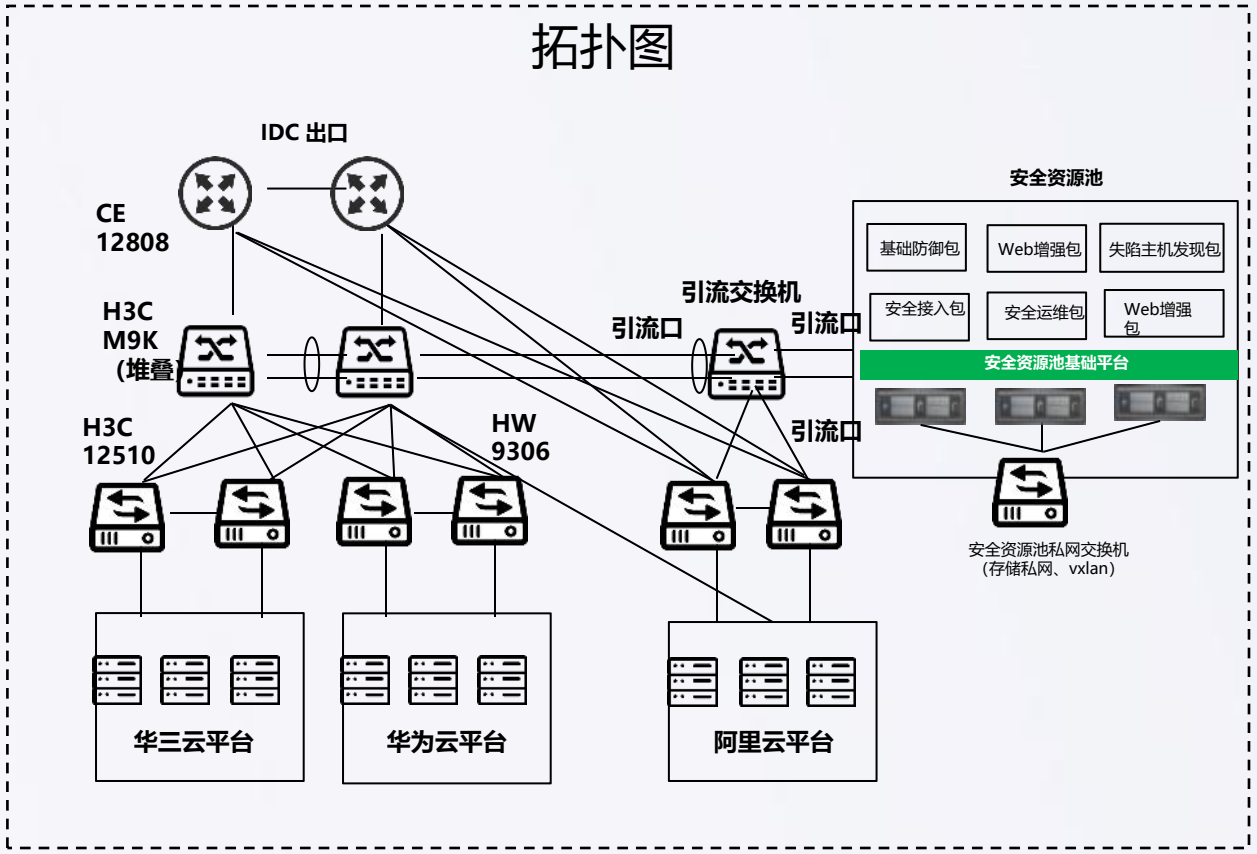
- ✓ 平台性能不足时，可以通过扩充标准服务器加入到集群中，保障平台性能
- ✓ 当用户分配安全服务性能不足时，亦可线性扩充性能

产品优势③：灵活开放　助力客户建立安全生态

品类	生态合作厂商
堡垒机	云安宝堡垒机、思福迪堡垒机、建恒信安堡堡垒机
终端安全	瑞星、卡巴斯基
网络准入	联软准入管理产品
数据安全	中安威士数据库安全产品
	美创数据库安全产品
日志审计	聚铭日志审计

客户价值

轻松上云，全过程防护，安全责任边界清晰



解决方案&价值

1. 通过一套安全资源池方案，为云平台**提供个性化，服务化的事前，事中，事后的细粒度的防御能力**；
2. **通过技术手段完善云上安全责任边界划分**，使云上安全责任、云上合规更易落；
3. **安全可视，交付简单**，在平台方界面向导式部署即可自动生成虚拟安全组件，全自动化的引流排版；
4. 支持为云上业务提供个性化，服务化的安全交付方案，**安全快速完成业务迁移**；
5. 租户对自身云上业务安全态势，实时可见、可控，打消上云顾虑；
6. 满足等级保护系列要求，达到合规建设的效果，为业务整合工作提供安全支撑；
7. 立体保护，实现”防、管、控”一体化的安全治理

部分成功案例

SANGFOR 深信服科技

省级政务云	市级政务云	私有云	运营商
北京市电子政务云	温州市电子政务云	葛洲坝集团务云	泉州移动
陕西省电子政务云	呼和浩特市电子政务云	华润集团	浙江省电信天翼云
山西省电子政务云	绍兴市电子政务云	四川省气象局	上海电信天翼云
安徽省电子政务云	台州市电子政务云	均瑶集团	江苏省联通IDC
海南省电子政务云	上饶市电子政务云	宝鸡市工商局	
	海口市电子政务云	中物物流	
	安徽省六安市电子政务云	温州市交通局	
	中山市电子政务云	四川省交通厅	
	佛山市电子政务云		
	武汉市新洲区电子政务云		
	武汉市武昌区电子政务云		
	佛山市三水区电子政务云		
	成都市温江区电子政务云		
	中山市电子政务云		

SANGFOR
深信服科技

SANGFOR 深信服科技

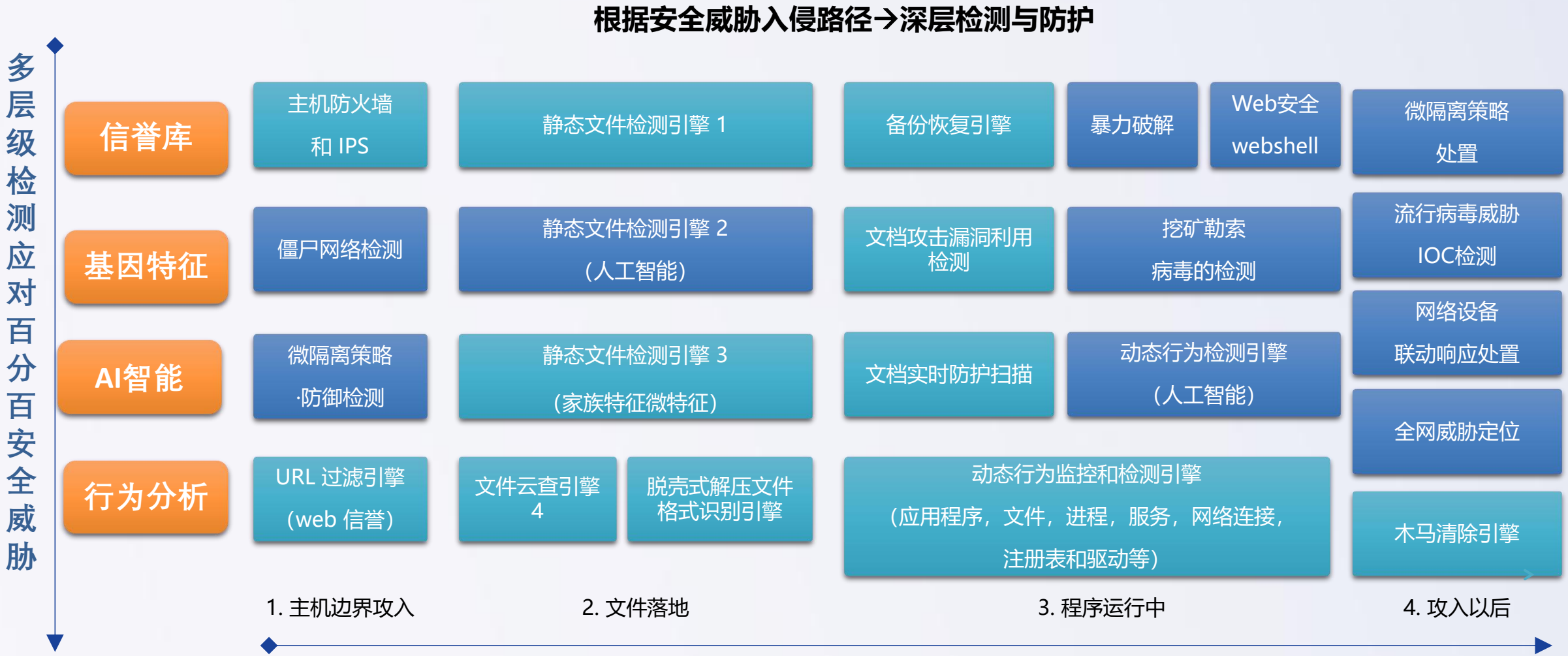
深信服智安全 SANGFOR SECURITY

终端检测响应平台EDR

EDR产品概述

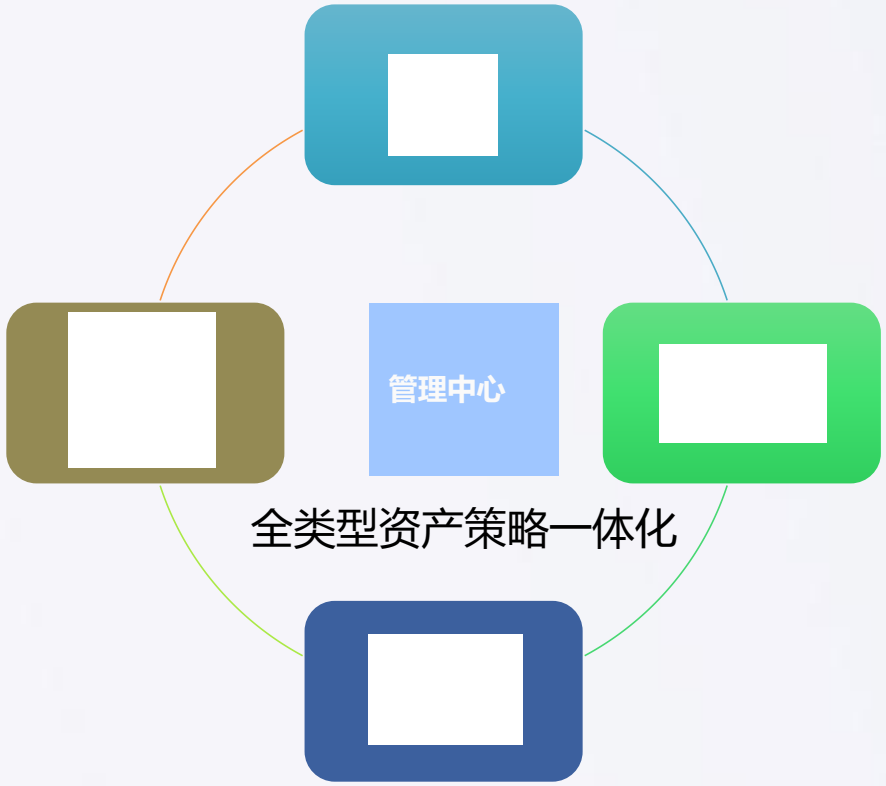
深信服终端检测响应平台EDR——围绕终端资产安全生命周期，通过预防、防御、检测、响应赋予终端更为细致的隔离策略、更为精准的查杀能力、更为持续的检测能力、更为快速的处置能力。在应对高级威胁的同时，通过云网端联动协同、威胁情报共享、多层级响应机制，帮助用户快速处置终端安全问题，构建轻量级、智能化、响应快的下一代终端安全系统。

优势点①：终端深层检测与防护



优势点②：支持全面的资产保护

全面保护、减少无效工作、体现运维工作价值



全类型资产策略一体化

全面检测防护手段

redhat®

SuSE

ORACLE LINUX

红旗® Linux

优势点③：快速响应 积极防御

云脑推送、接收热点事件威胁情报

威胁上报与接收

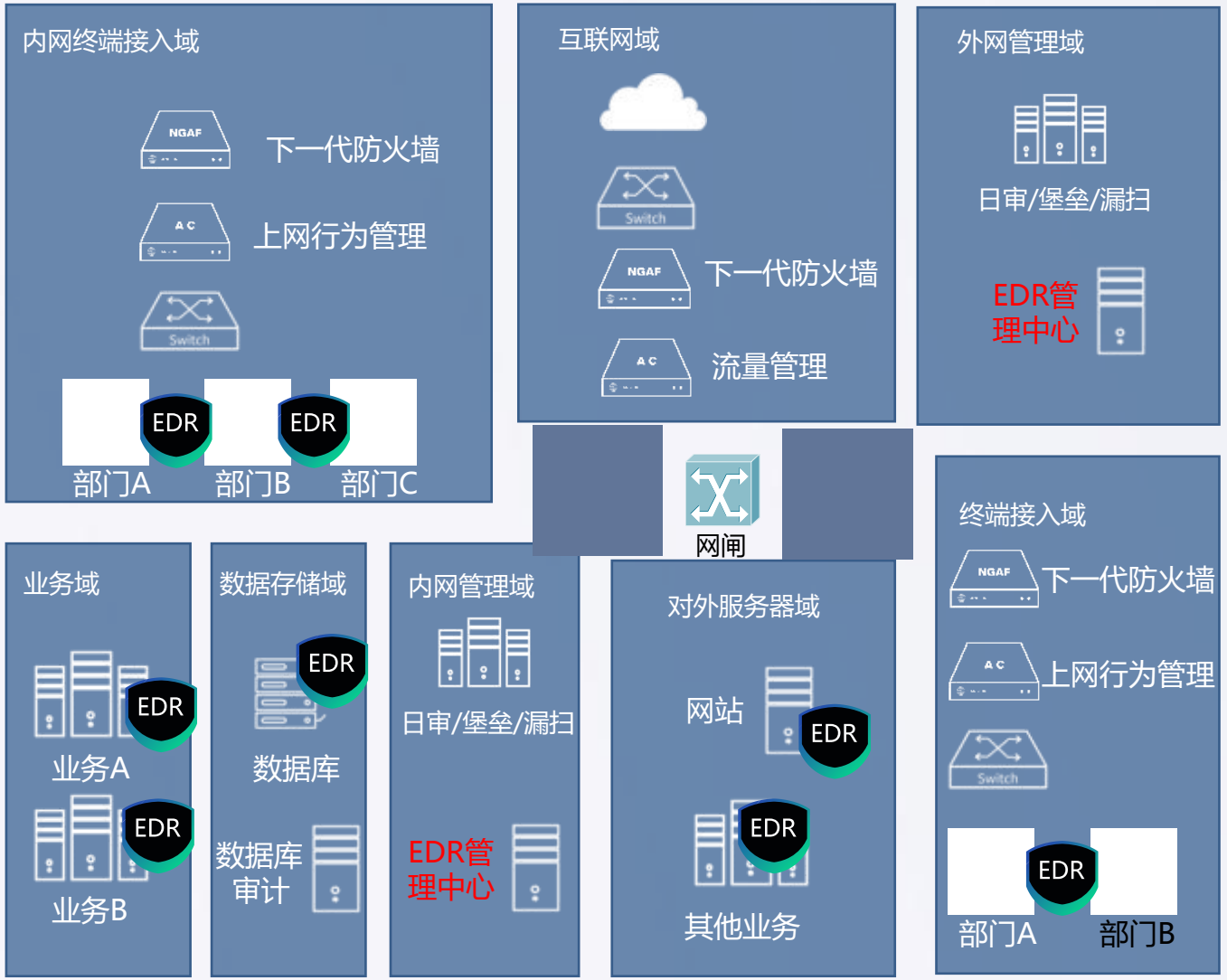
任务指令推送

威胁上报与接收

威胁情报接收自动处置

极大缩短威胁驻留时间

应用场景一 等保合规场景



01 政策合规

贴合国家政策法规，满足主机恶意代码防范要求，基线检查，确保终端安全合规

02 分域保护

对各区域实施安全保护措施形成立体的安全保护体系

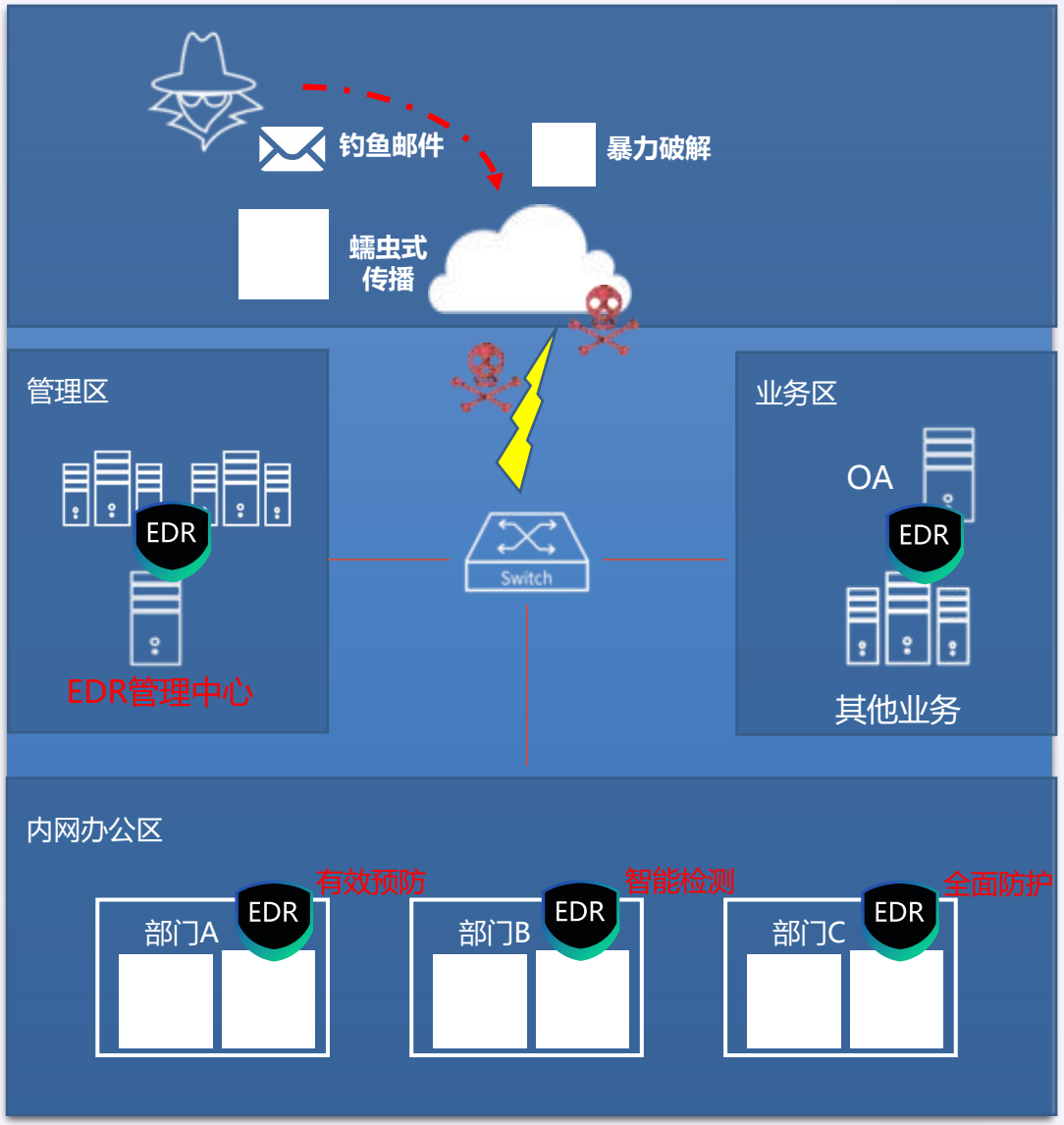
03 有效防护

对终端进行全面防护，有效应对已知、未知、高级威胁

04 能力提升

安全不止合规，持续输送防护+管控+检测+响应安全能力

应用场景二 未知威胁防护



01 **有效预防**

账号及密码策略排查

全网威胁展示与定位

基于最小授权原则，做不同业务、不同终端隔离访问控制

02 **全面防护**

处置暴力破解、WebShell、僵尸网络等威胁

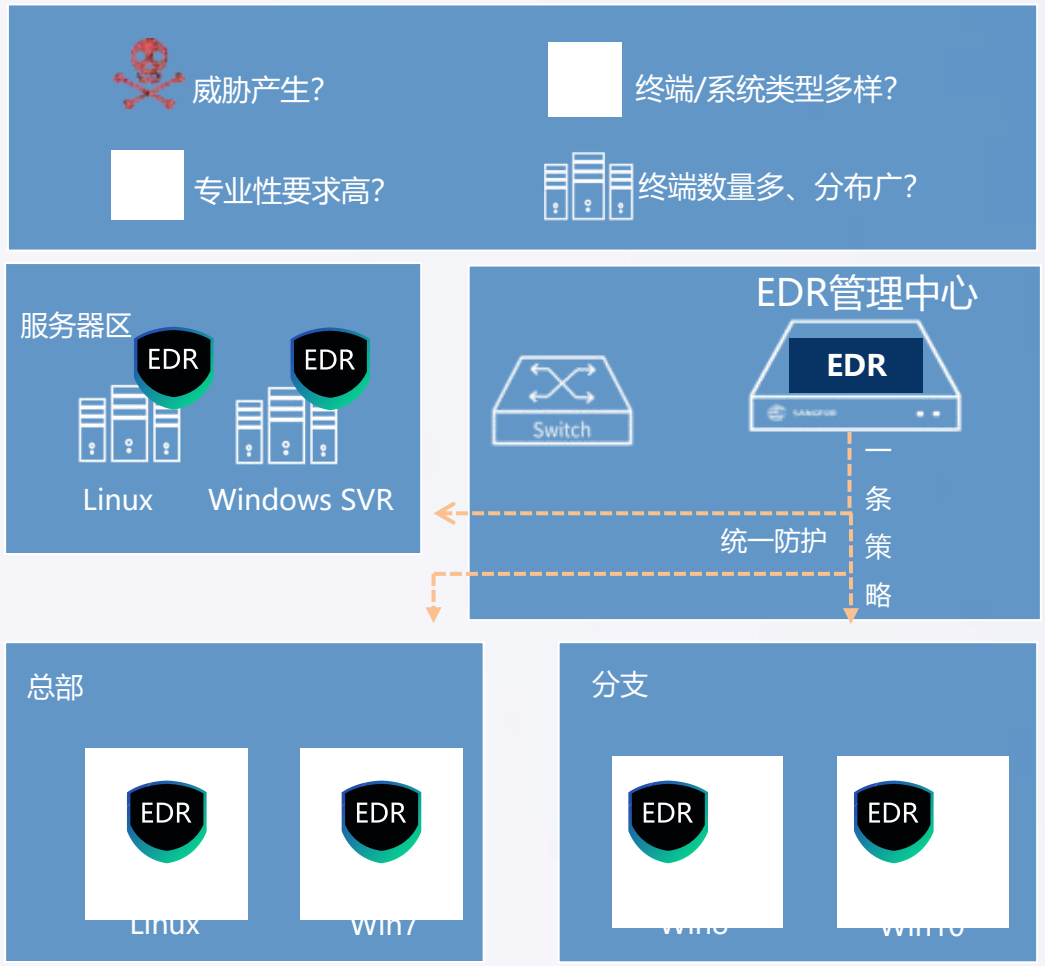
03 **智能检测**

利用人工智能SAVE引擎，无特征技术，对未知威胁进行实时检测

深信服人工智能检测引擎SAVE

SANGFOR AI-based Vanguard Engine

应用场景三 企业级运维场景



01 **全面防御**

多维度持续威胁检测、响应，有效威胁防御，杜绝威胁产生，减免不必要维护成本

02 **统一维护**

资产统一维护，责任落实到人，风险快速定位

03 **便捷管理**

不区分终端/系统类型，一体化策略下发，自动执行

04 **快速处置**

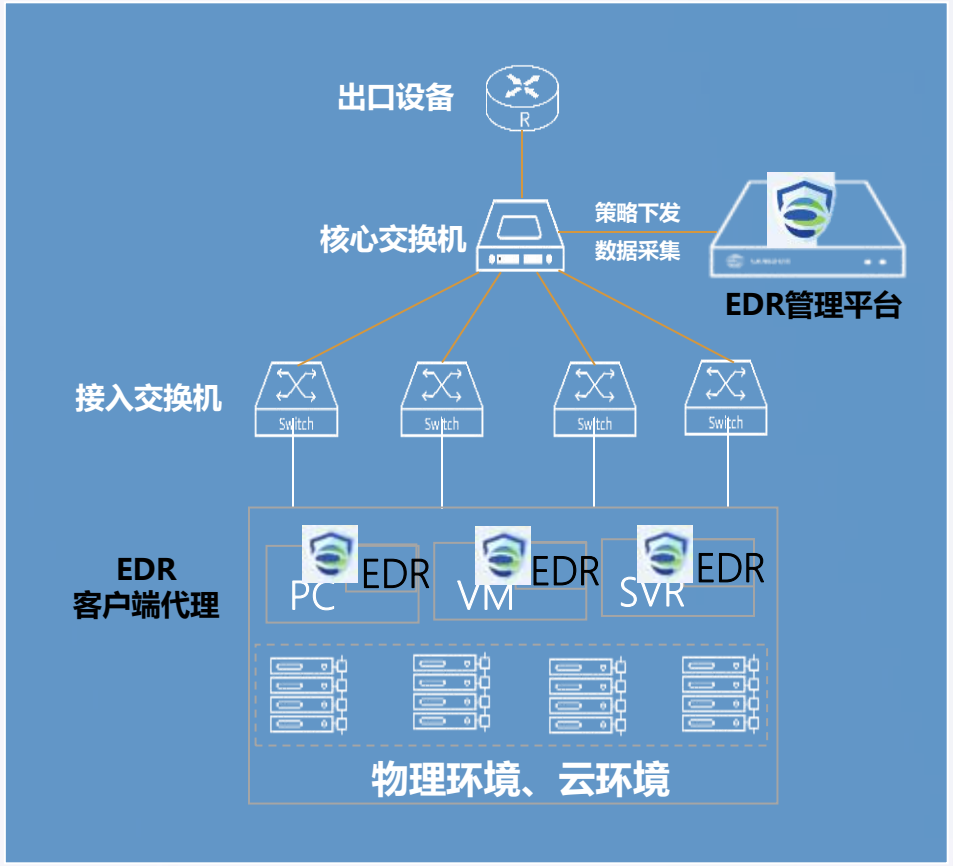
一键终端隔离、自动隔离

一键文件隔离、修复

自动响应，协同联动处置

应用场景四 终端安全保护场景

支持传统PC、物理服务器、虚拟机、云主机等场景的终端保护



- ✓ 赋予用户持续进化的预警、防御、检测与响应能力
- ✓ 为IT和业务提供持续保护，让安全建设更有效、更简单！
- ✓ 虚拟化底层平台解耦合，构建动态安全边界

- EDR=Endpoint Detection Response
  智能检测、灵动响应、全面保护
- 系统为C/S部署、B/S管理方式
  无需对网络进行调整或对网络设备进行配置
- 运用AI智能、信誉库、基因特征、行为分析全面应对威胁
  文件/主机/联动，多维度威胁响应处置
  广泛适配辅以多角度防护措施，确保终端全面保护

EDR产品案例介绍

政府	企业	教育	医疗
国家互联网应急中心cncert/cc	国家电网有限公司	山东大学	广西医科大一附院
中华人民共和国国家卫健委	京东方有限公司	南方科技大学	淄博市妇幼保健院
浙江省体育局	康佳集团股份有限公司	云南师范大学	安徽中医药大学第二附属医院
广西省公安厅	膳魔师（中国）股份有限公司	武汉轻工大学	河池地区人民医院
内蒙古经信委	中国联合航空有限公司	宁夏理工学院	怀化市第一人民医院
上海市环保局	福耀玻璃工业集团股份有限公司	辽宁财贸学院	胶州市中心医院
山西省水利厅	中国高新投资集团	中国大连高级经理学院	四川省人民医院
新疆自治区安监局	中铁城建集团有限公司	河北环境工程学院	广西医科大一附院
西藏自治区交通厅	华侨城集团	山东药品食品职业学院	东莞市卫生局
新疆自治区公安厅	中国国电集团	山东职业学院	北京市西城区卫生局
天津市环保局	绿地集团	南宁职业技术学院	张家口市卫生局
公安部一所	华润(深圳)有限公司	广西幼儿师范高等专科学校	长沙市卫计委
新疆自治区司法厅	国贸控股有限公司	桂林医学院	南京市溧水区卫生局

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

企业移动管理EMM

深信服EMM产品概述

深信服企业移动应用管理EMM

- ✓ 支持企业移动业务的全方位数据安全保护；
- ✓ 统一的移动安全工作域，与个人域完全隔离，防止终端侧恶意泄密；
- ✓ 移动应用网络接入传输全程加密，防止信息监听与篡改；
- ✓ 移动应用服务器隐藏，数据封闭保护；
- ✓ 兼容性强，推广和使用简单、易用。

定位	**移动化安全工作空间** 移动业务发布　　移动数据安全
客户价值	让办公 安全的延伸 到移动端，提升 办公效率，开展业务创新，提升IT价值。

深信服EMM三大方案

深信服提供面向客户场景的三种企业移动应用安全管控方案

EasyApp
（接入安全）

- 业务系统防护
- 接入安全

注：按并发授权数收费

EasyWork
（接入安全 + 终端数据安全）

- 业务系统防护
- 接入安全

注：VPN功能可以不开启，但虚拟网卡依旧会启动，用于提供终端网络隔离保护能力。

- 应用发布
- 应用推广
- 终端环境检测与准入
- 应用层双域隔离
- 应用安全报表

注：按终端注册数收费

EasyWork+
（接入安全 + 终端数据安全 + 终端安全）

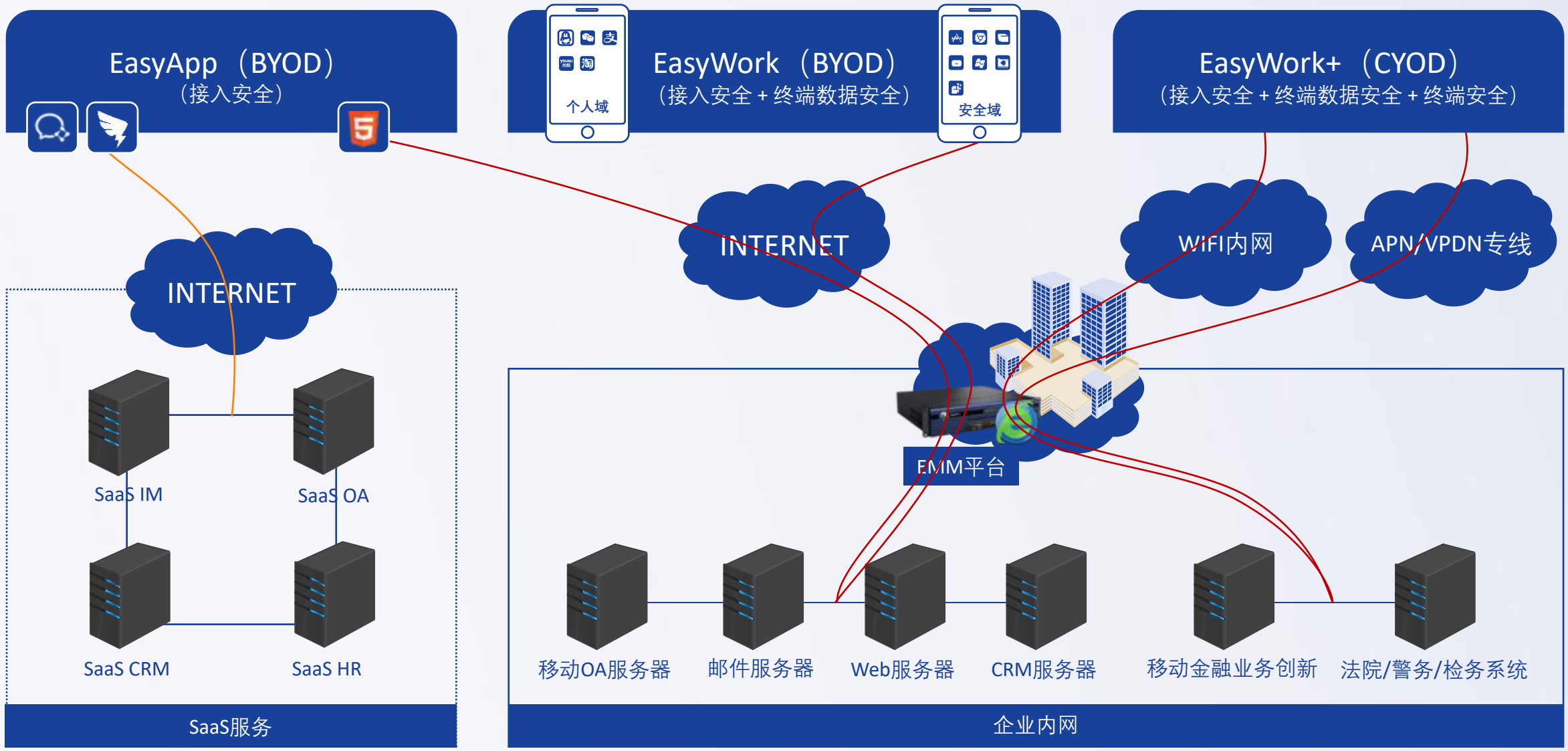
- 业务系统防护
- 接入安全

注：VPN功能可以不开启，但虚拟网卡依旧会启动，用于提供终端网络隔离保护能力。

- 应用发布
- 应用推广
- 终端环境检测与准入
- 应用层双域隔离
- 应用安全报表
- 设备层强管控
- 系统层专机专用

注：按终端注册数收费

深信服三大方案组网架构



方案优势

最安全

- ✓ **9 种身份认证方式：**用户名/密码、硬件特征码、短信、动态令牌、USB KEY、CA、LDAP、Radius、口袋助理动态码认证
- ✓ 主从账号绑定：如果销售登录的是自己的远程接入账号，即便他盗取了老板的业务系统帐号，也没办法登录。
- ✓ 最细致的权限划分：按角色划分访问权限，销售管理系统可以 让销售访问、财务系统只能财务访问，而老板则可以访问所有系统

最快速

- ✓ **多线路智能选路：**多条线路同时接入的情况下，自动选择最快 的线路接入。默认是移动走移动、联通走联通、电信走电信。
- ✓ 单边加速和高速传输协议：占满带宽传输工作文件，打开系统 速度更快
- ✓ 流缓存：削减 75% 左右的重复流量，即可降低四分之三的文件 传输工作，用 1 分钟的时间传输 4 分钟才能传完的数据，提升效率

最易用

- ✓ **系统兼容性强：**兼容 Windows、MAC 和 Linux 系统
- ✓ 浏览器兼容性：兼容所有浏览器
- ✓ 移动终端兼容性：支持 Android 和 IOS 最新版本智能终端

可扩展

- ✓ **系统扩展性强：**所有的 Windows 应用， 可直接平移到 Windows、MAC、Android 和 IOS 终端上，不用做任何开发
- ✓ 移动APP封装：在 APP 中直接植入安全接入代码，只安装移 动办公 APP 即可完成远程安全登录过程，用户使用更简单

客户价值-移动办公数据防泄密场景

SANGFOR 深信服科技

全方位一体化解决业务发布问题和安全建设问题

客户价值- 政务微信数据防泄密场景

保护自建H5应用的传输安全；保护H5业务服务器不被扫描攻击；提供国家商用密码算法更合规

INTERNET

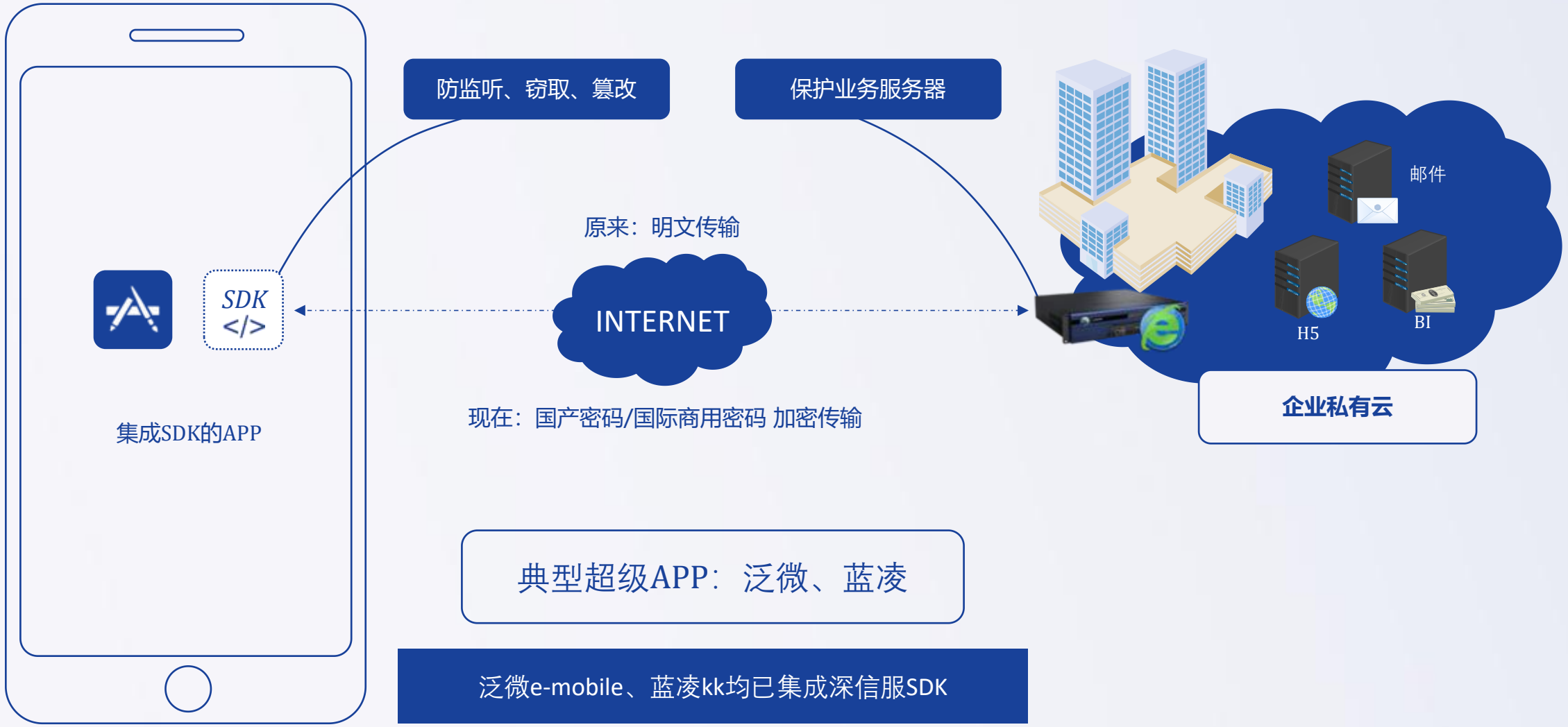
政务微信提供强大稳定的IM通讯能力、通用OA能力，大幅提升办公效率。

1. 部署灵活，支持多网络部署，适配各网络环境。
2. 安全可控，满足政府机构对数据安全的要求。
3. 平台强大，产品操作体验与微信一致，免培训。
4. 连接微信，为民生服务等场景的延展提供丰富可能

移动数据安全

防拍照	防复制	防截屏	防分享	防拷贝	防网络外发	防离职带离数据
防恶意代码	防APP漏洞	防病毒	防恶意WIFI劫持	防钓鱼		

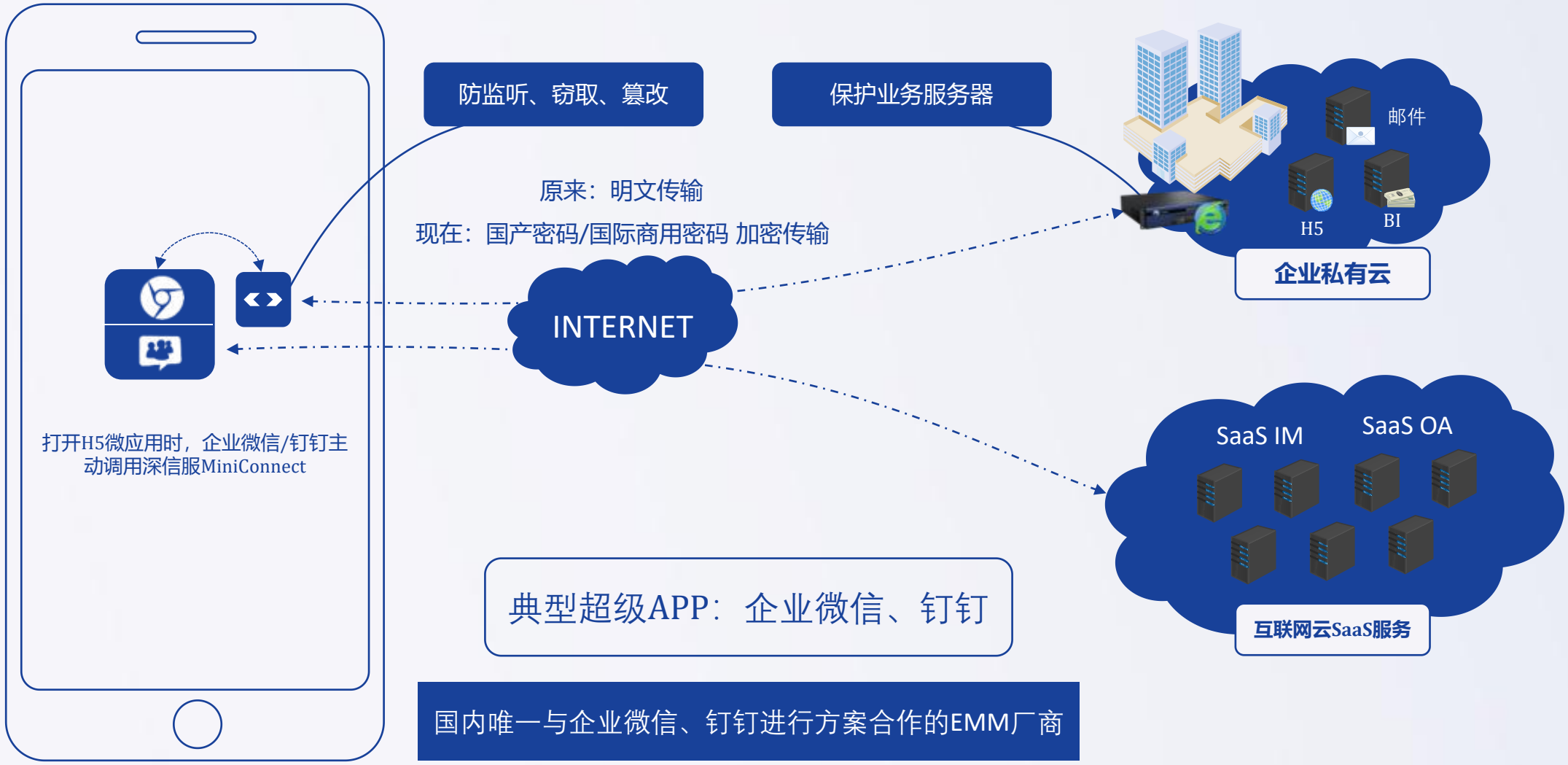
深信服EMM - 超级APP场景



典型超级APP：泛微、蓝凌

泛微e-mobile、蓝凌kk均已集成深信服SDK

客户价值-超级APP场景



典型超级APP：企业微信、钉钉

国内唯一与企业微信、钉钉进行方案合作的EMM厂商

客户价值-专机专用 & 等保合规 场景

单桌面模式	适用于移动金融业务创新等生产场景。
双桌面模式	适用于政府、公安、法院等保合规场景。

基于CYOD移动设备

厂商深度集成方案

支持华为EMUI 5.1及以上版本

小米手机正在深度集成中

融合通用方案（含Android DeviceOwner和多种辅助技术）

支持Andorid 5.0及以上版本的主流厂商手机

部分典型客户

政府	金融	企业	区域政府	公安/委办	军队/运营商
国家体育总局	邮储银行总行	深圳市水务集团有限公司	扬州市政府	湖南长沙市公安局	人民解放军东部战区
河北质量技术监督管理局	成都市农商行	福建省高速公路有限公司	武昌区政府	四川成都公安局成华分局	人民解放军驻杭州某部队
江西人力资源与社会保障厅	青海银行	山东鲁西化工股份有限公司	新疆自治区政府	天津西青区公安消防支队	人民解放军驻锦州某部队
广西壮族自治区地方税务局	中国农业银行	金鹰卡通	贵州市政府	福建海事局	江苏电信
河南省地震局	青岛银行	山西省烟草专卖局	山东德州区政府	福建省出入境检验检疫局	云南移动
上海出入境检验检疫局	中国银行	万科集团	余杭区政府	南昌市铁路局	江西联通

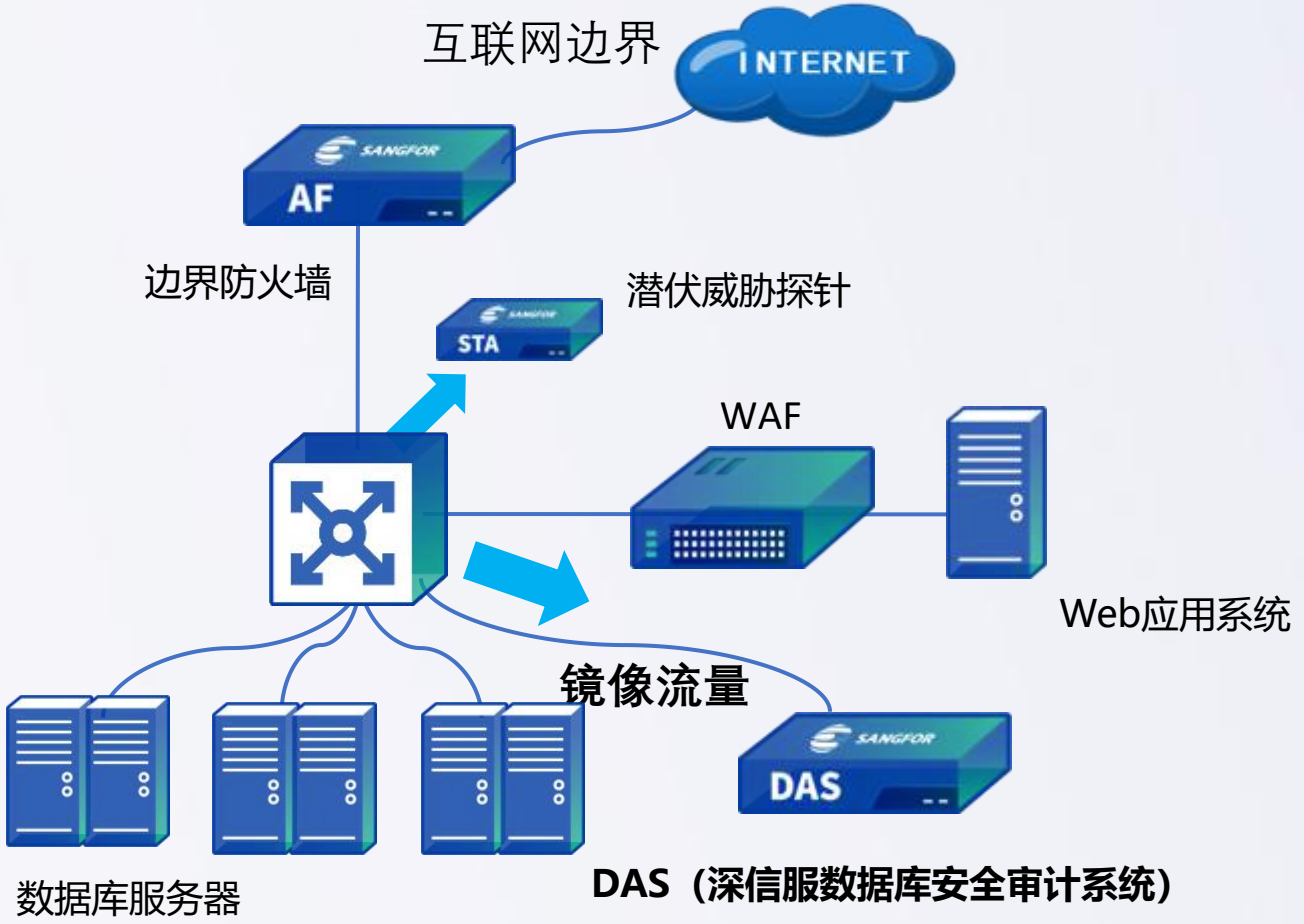
SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

数据库审计DAS

产品概述

深信服数据库安全审计系统DAS（Database security Audit System ）是深信服基于对用户数据资产防护的不断探索，创新地将数据安全防护与大数据分析结合的产物，它能为用户提供完整的数据库审计分析、泄密轨迹分析、数据库访问关系可视、数据库攻击威胁分析等价值。



产品优势

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

数据库访问可视

系统具备可视化分析视图并提供交互式分析工具帮助用户及时发现数据库危险

审计日志秒级查询

自主研发的高性能数据库，在保障数据高可靠性的同时，提供秒级查询、日志事物重做

数据库口令爆破检测

系统具备自动生成口令爆破的动态规则，防止攻击者爆库操作

贴合运维需要，实用性强

A 系统具备新型SQL新模板的趋势图，方便结合web日志快速还原黑客入侵的行为操作和轨迹

B 根据SQL语义语法自动生成SQL模板以提高审计性能，优化展示输出，直观呈现风险

联动互联网边界组件

系统具备与边界产品联动（例如AC、AF），以帮助有效发现潜在威胁 如：webshell数据窃取、泄密分析等

支持多维分析与报表输出

支持多维分析、自定义报表、SQL模板分析等全面强大的报表功能。比友商更全面、易用、可视。

应用场景①：数据泄密分析

互联网

AC

数据安全系统

Switch

姓名	工资	手机号	社保卡号
陆明友	3044	18691695196	166599079
何海生	3781	18621044328	257002355
张文涛	4961	18673175897	309758157
林国强	3501	18674228529	284913326
张盛泰	4927	18688497370	444513291

应用服务区

前置机

Web

中间件

数据存储区

DAS

ID	UserName	Salary	PhoneNumber	SocialID
22747	陆明友	3044	18691695196	166599079
22748	何海生	3781	18621044328	257002355
22749	张文涛	4961	18673175897	309758157
22750	梁景波	4157	18660206569	425536139
22751	阳海斌	4744	18699442040	240811794
22752	朱隽	3671	18647842064	446836753
22753	林国强	3501	18674228529	284913326
22754	张盛泰	4927	18688497370	444513291

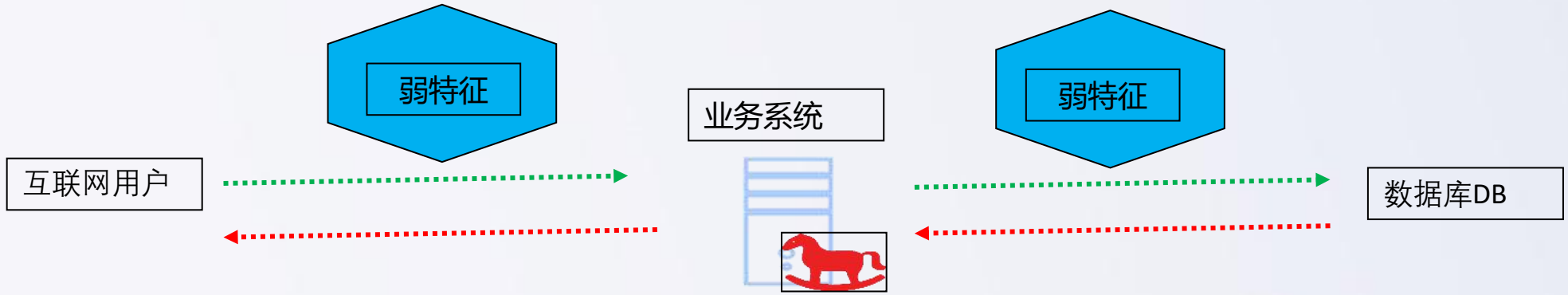
数据库（群）

办公区

运维区

应用场景①：数据泄密分析

应用场景②：数据窃取分析



GET mywebshell/echo.php

200 OK

id	name	statue
424	Zhujun	working
425	lmy	traveling

select* from users

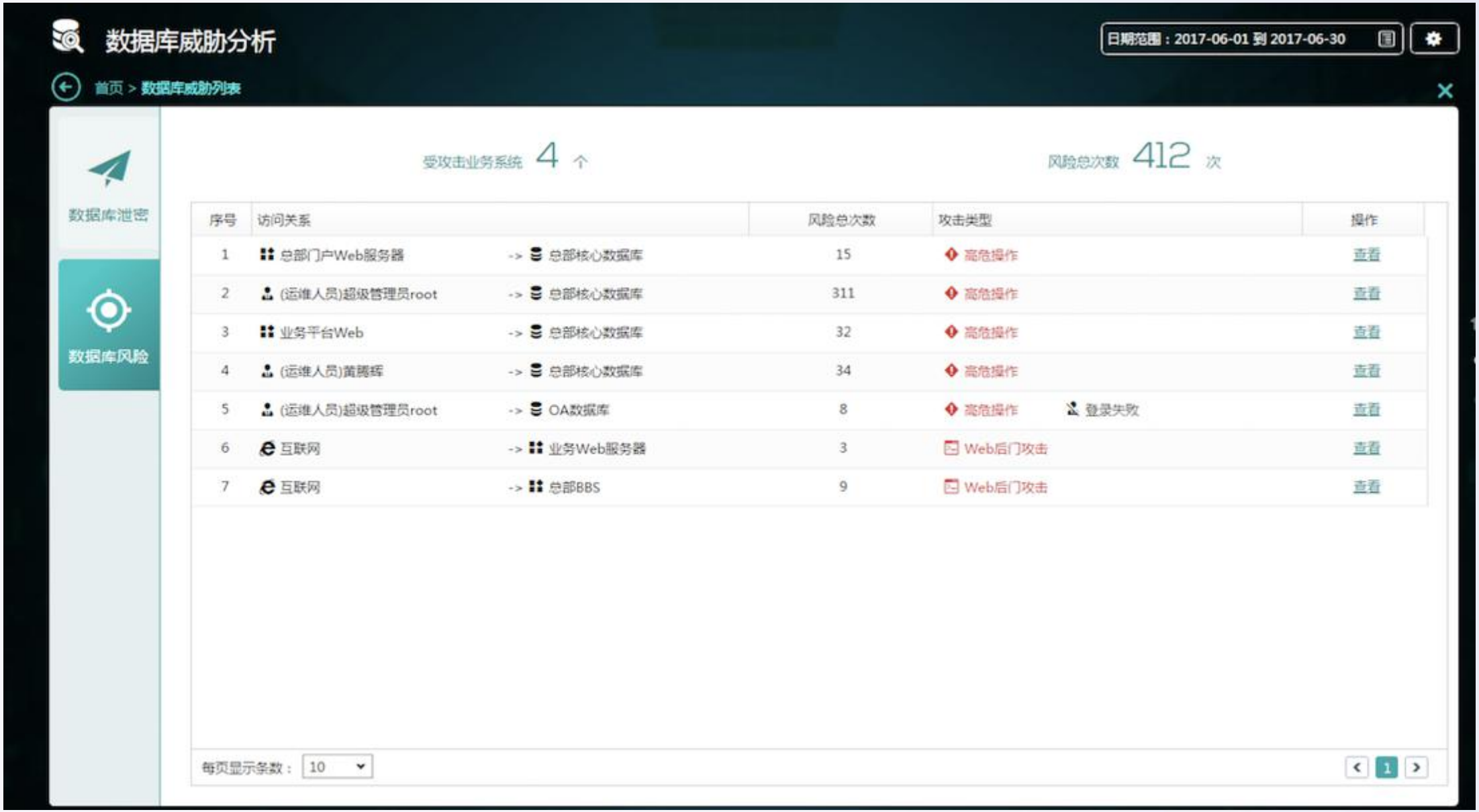
id	name	statue
424	Zhujun	working
425	lmy	traveling

关联分析
强特征

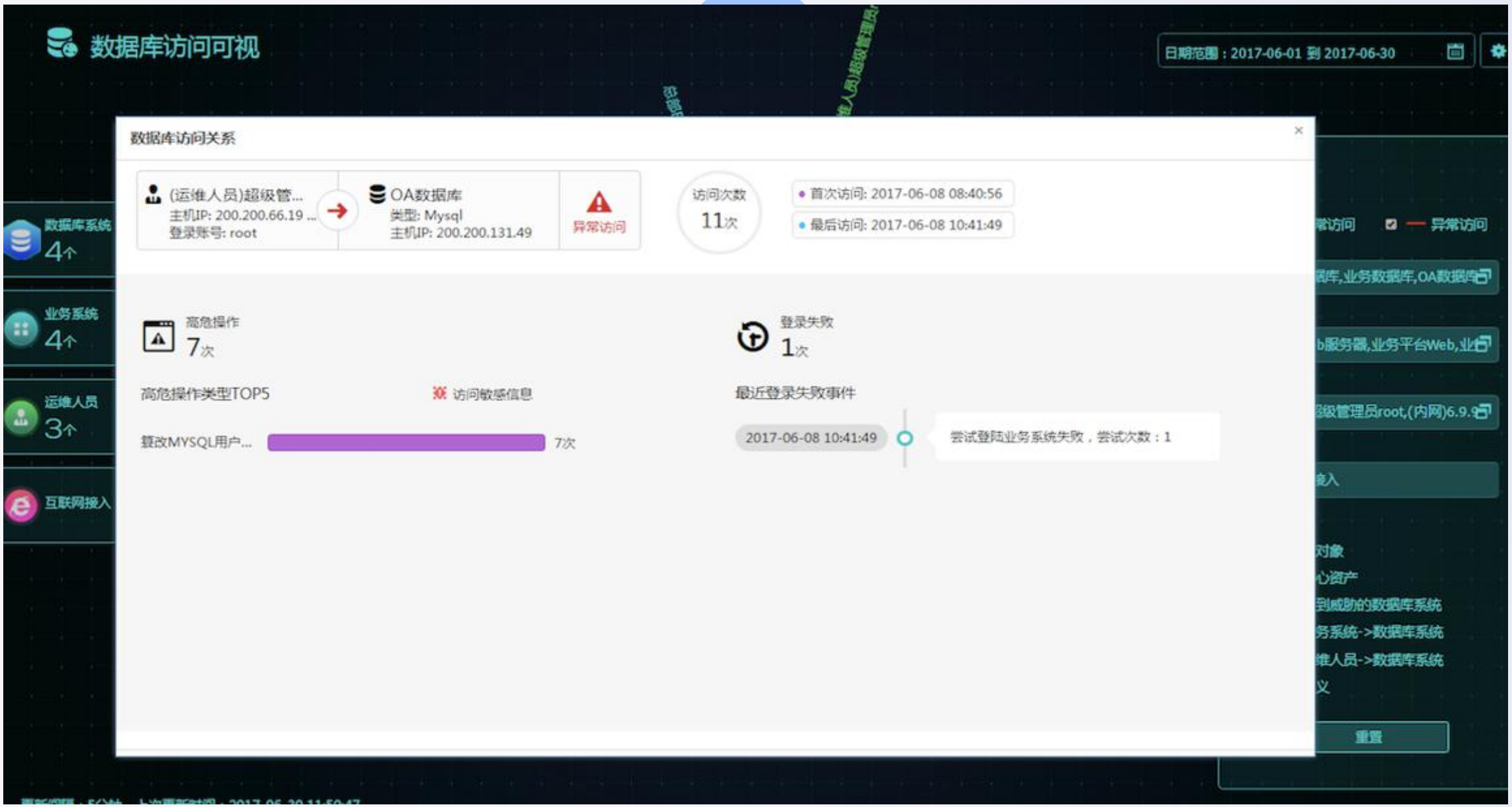
联动检测

联动封锁

应用场景②：数据窃取分析



应用场景③：用户行为分析可视化



SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

桌面云aDesk

深信服桌面云aDesk产品概述

- 新一代终端建设目标，包括三点：第一，简化运维，需要快速完成平台搭建和资源方法，并且能够简化系统和应用的管理、以及减少现场维护的次数，提高运维效率；第二、需要保证数据的安全，无论是数据安全不丢失，还是数据安全不泄露；最后，是要能够有效降低TCO，无论是通过降低运维管理成本还是硬件维护成本。
- 在此需求背景下，就诞生的桌面云产品，它是一种替代PC的理想方案，通过将桌面上云，可以将原来绑定在PC上的桌面、应用和数据全部迁移到数据中心，然后通过虚拟交付协议将操作系统界面以图像的方式传送给前端的接入设备，包括云终端、笔记本、普通PC、智能终端等，这种桌面资源集中化的部署方，以及软硬件解耦的架构，就可以有效解决前面讲到的安全、运维和成本的问题。

深信服桌面云“云、网、端”架构

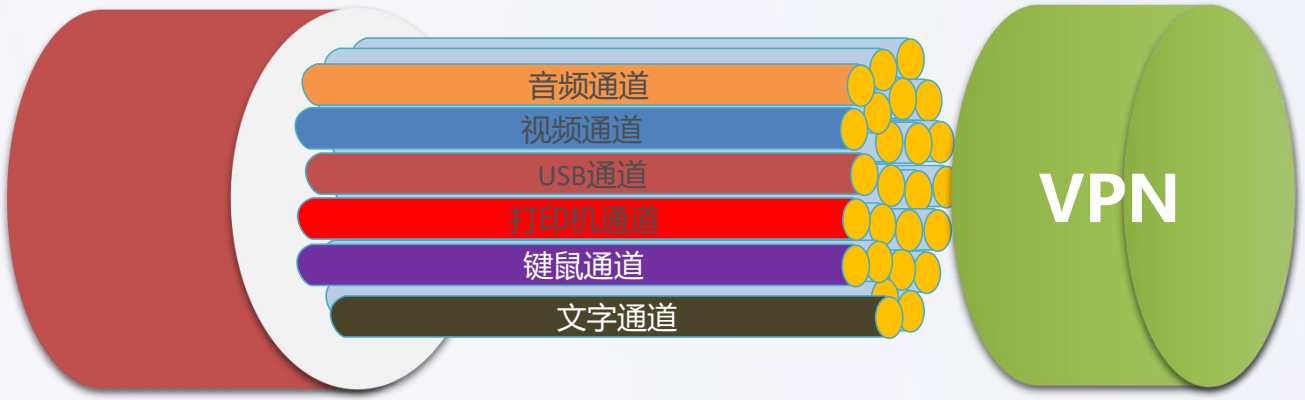
云：VDS超融合一体机预集成

服务器虚拟化　存储虚拟化　桌面虚拟化　GPU虚拟化

VDS桌面云超融合一体机

- ❑ 开箱即用
- ❑ 基于超融合架构
- ❑ 高可靠性设计
- ❑ 支持线性扩容

网：自研高效交付协议



- HEDC高效能桌面编码
- “零总线外设映射”
- 细粒度传输通道，内置VPN加密
- 基于体验感知自适应压缩策略

端：aDesk瘦终端零运维，绿色节能

普通办公/2D设计

ARM瘦终端

双屏显示/3D设计

X86瘦终端

PC利旧/安全隔离

台式电脑

PC利旧/移动办公

笔记本电脑

移动办公

手机/平板

- ❑ 设备故障率低，终端集中管
- ❑ 低功耗设计,绿色节能噪音少

- ❑ 可利旧PC，保护客户现有资产
- ❑ 构建无边界移动安全办公环境

产品优势

深信服aDesk深度融合桌面云

流畅度
媲美PC

极致体验

01

极简架构
运维自动化

高效

02

简单、敏捷
的安全

安全

03

通过前后端软硬件的深度融合，交付极致体验，更安全、更高效的桌面云。

深信服桌面云方案介绍

普通办公

安全办公

软件开发

分支办公

第三方人员外包

呼叫中心

生产线场景

图形设计

遍布全国的高端客户案例

企业	FOXCONN 富士康科技集团	Hisense	BYD 新能源汽车 引领者	兖矿集团 YANKUANG GROUP
政府	中华人民共和国文化和旅游部 MINISTRY OF CULTURE AND TOURISM OF THE PEOPLE'S REPUBLIC OF CHINA	江西省人民检察院 www.jx.jcy.gov.cn	南京市公安局 Nanjing Municipal Public Security Bureau	甘肃省高级人民法院
教育	北京大学 PEKING UNIVERSITY	武漢大學 WUHAN UNIVERSITY	西南大學 SOUTHWEST UNIVERSITY	河北衡水中学
金融	中国人民银行 THE PEOPLE'S BANK OF CHINA	华夏银行 HUAXIA BANK	深圳农村商业银行 Shenzhen Rural Commercial Bank	深圳证券信息有限公司 Shenzhen Securities Information Co., Ltd.
医疗	山西省中医院 山西省中医药研究院	China Meitan General Hospital 煤炭总医院	泸州市人民医院 LUZHOU PEOPLE'S HOSPITAL	天津市第三中心医院 Tianjin Third Central Hospital

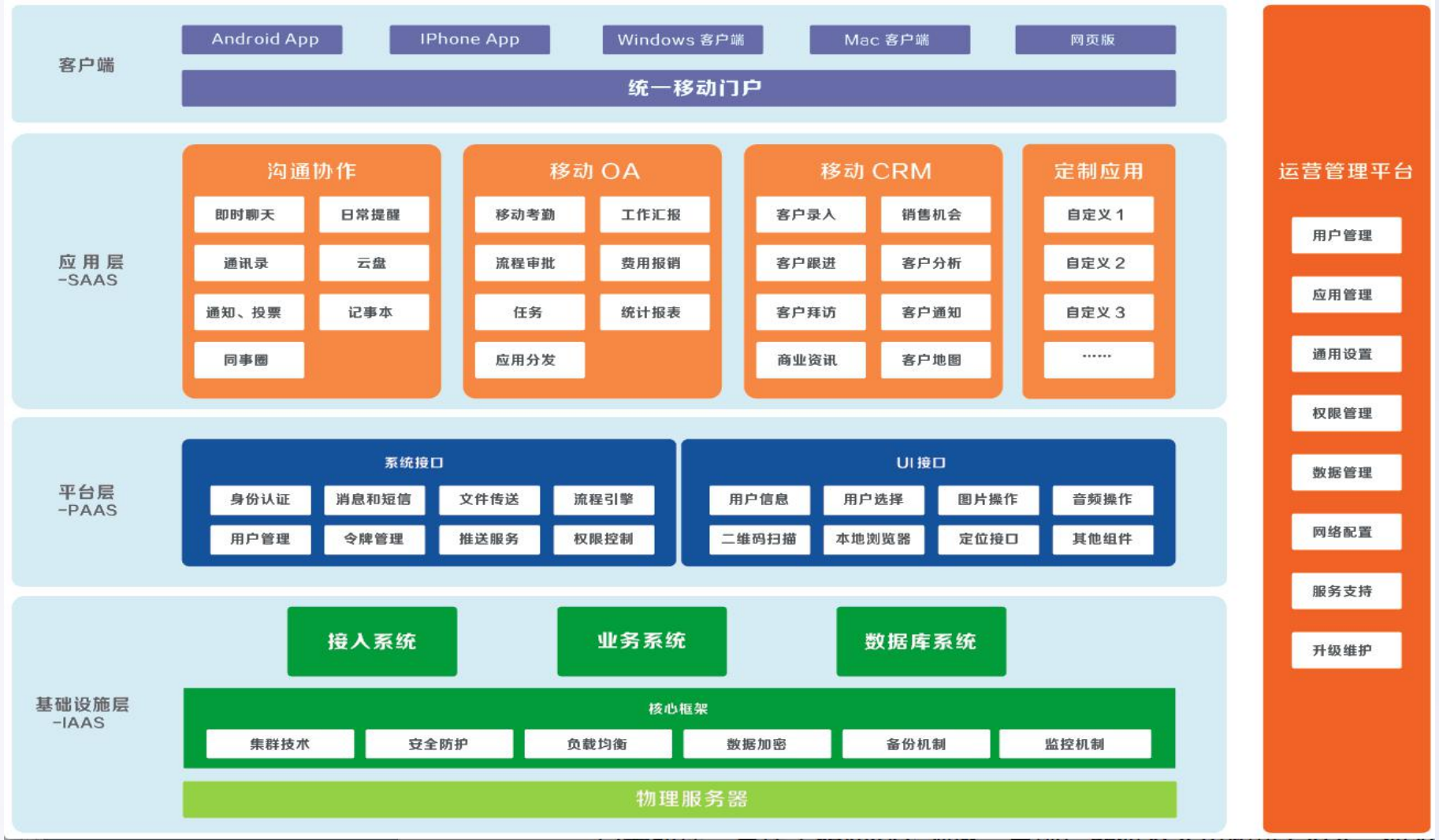
已服务中国文化部、江西省检察院、富士康集团、海信集团、中国银行、山西省中医院、北京大学等用户，案例超过 6,000 家

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

口袋助理

口袋助理产品概述

针对政府、金融、企业、教育等用户的移动办公需求和安全需求，口袋助理提供一套完善的移动办公解决方案，使得单位领导、成员在任何时候、任何场所，通过手机里的口袋助理APP就可以实现移动考勤、流程审批、发布通知、即时沟通、与单位现有各系统对接等，帮助提高工作效率，统一管控，减少IT人员的运维和管理难度。



口袋助理产品价值

SANGFOR 深信服科技

单位通讯录：组织架构一目了然 轻松找到责任人 分级权限保护领导隐私

内部工作群组：一秒创建工作小组 高效完成沟通合作 避免工作信息泄露

即时通讯：文件传输、语音、已读未读@功能，让沟通更高效

考勤：智能签到，员工上班、迟到、早退、请假等清晰可见

审批：不受时间、空间限制，审批效率提升95%

邮件：出差、开会、外出调研，在手机上也能收发邮件

签到：支持WIFI签到、外勤签到、上下班签到

通知：公文的上传下达，已读未读提醒评论让通知传达更高效

云盘：文件保存、共享、调用，查看更便捷

工作汇报：在手机完成工作记录及汇报

智能报表：智能报表分析，让统计、管理更简单

开放平台：轻松接入已有业务系统

统一的工作平台：移动办公门户，统一入口，统一管理，降低维护成本，提升使用体验

私有云部署：所有信息存储在本地服务器，更安全可控

口袋助理产品价值—产品界面展示

SANGFOR 深信服科技

产品下载地址：http://www.kd77.cn

SANGFOR 深信服科技

2000000家+企业的共同选择

SANGFOR
深信服科技

SANGFOR 深信服科技

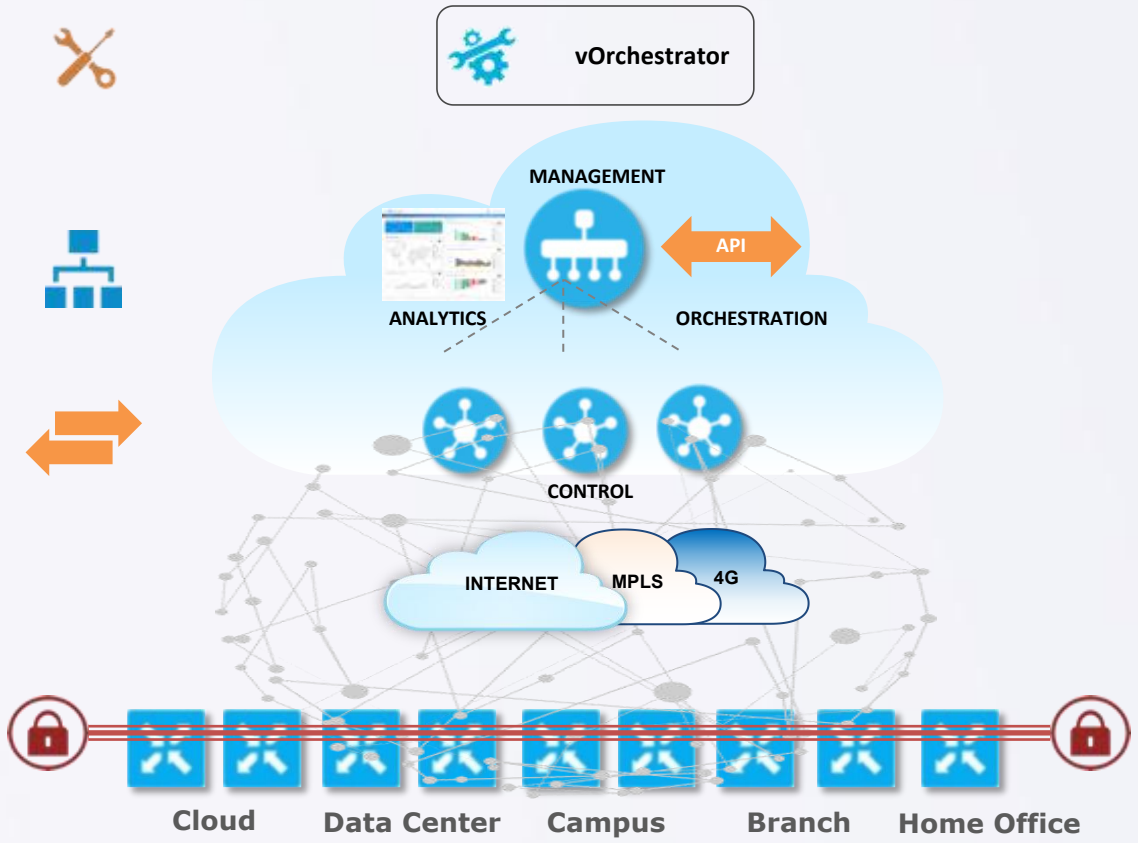
深信服智安全 SANGFOR SECURITY

广域网 SD-WAN

SDWAN产品概述

业务转型，网络是关键，当前组网的三大挑战，分别是：（1） **WAN流量激增，扩容带宽成本高，访问体验差；（2）基于公网访问体验不佳，多云、多分支运维复杂；（3） 跨境组网成本高昂，VPN组网访问体验差。** 基于此，新型WAN需要具备三大特性：

1、多WAN接入并智能选路，综合利用多条共有或私有链路，让普通链路能够达到专线的网络质量，降低了流量成本，提高了带宽；
2、快速灵活部署，SD-WAN 支持设备即插即用的易部署，只需部署边缘设备，设备即可通过集中管理设备自动下载指定配置和策略，实现简灵活部署；
3、网络集中管理，SD-WAN 通常会提供集中管理系统，用于网络多设备配置、WAN 连接管理、应用流量设置及网络资源利用率监控等，以此达到网络简化管理和故障排查的目的。



管理平面

智能应用识别、安全/运维策略统一管理、设备统一管理、全网统一监控、AUTO VPN、NFV业务编排等

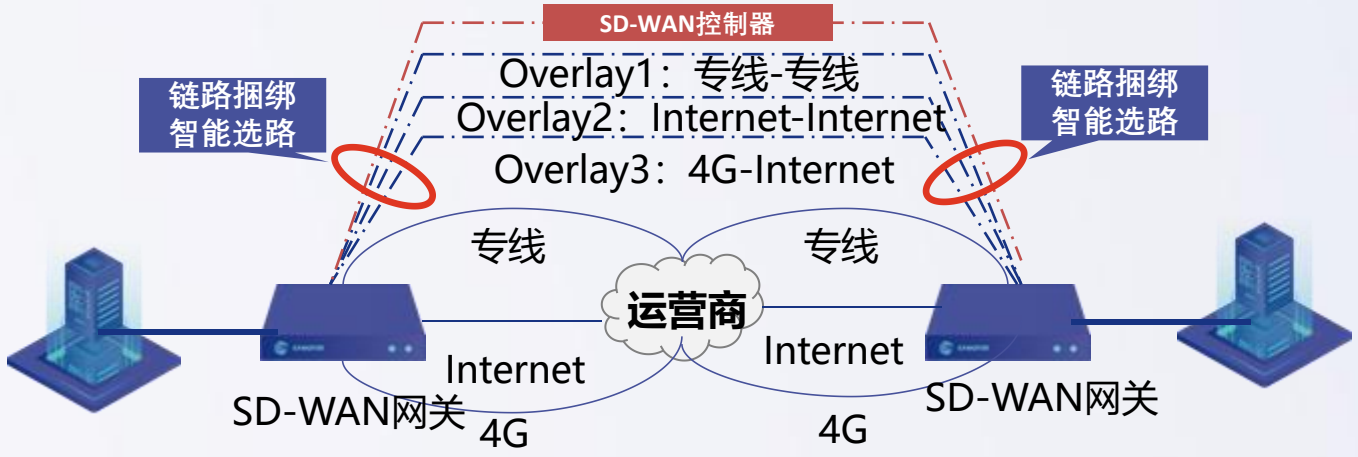
控制平面

智能选路、智能QOS、overlay隧道、TCP/UDP广域网传输优化、NFV安全等

数据平面

多WAN接入、多WAN池化、多WAN捆绑等

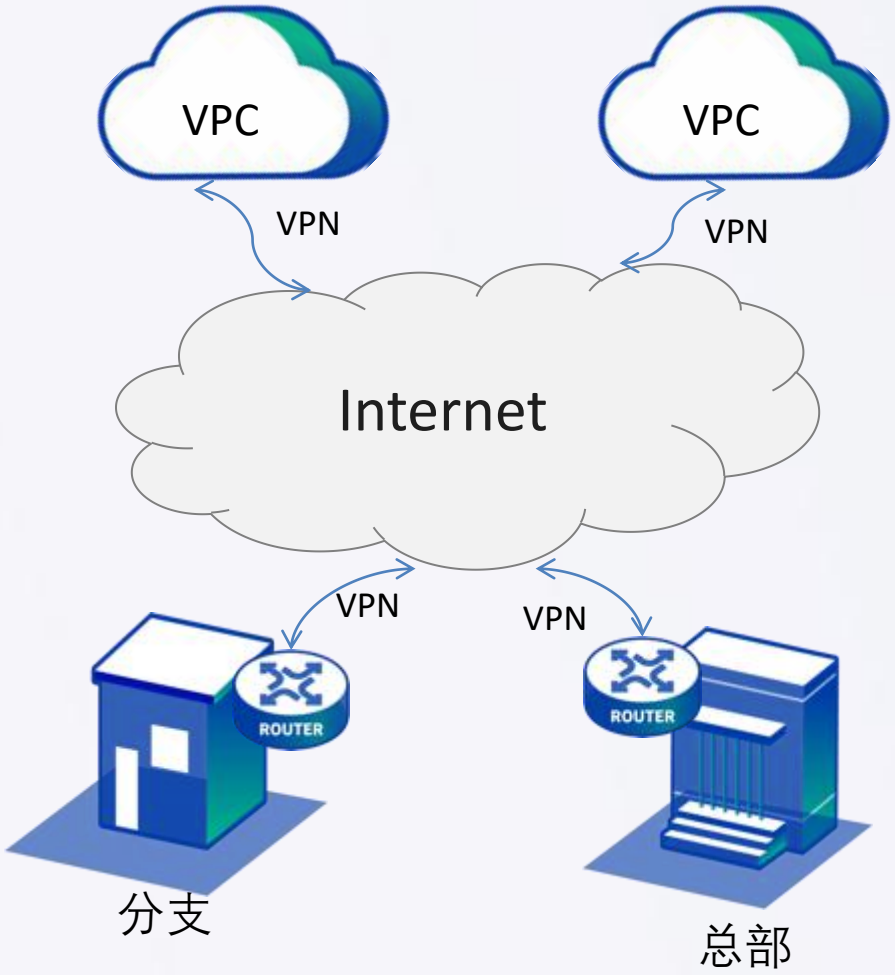
特性1：引入更便宜的互联网搭配专线
为业务提供差异化服务，达到降低线路成本同时提升核心业务体验及连续性



SD-WAN降低线路成本思路:

- **引入互联网，形成专线+互联网**（VPN+4G），为不同业务提供不同质量链路资源
- 通过SD-WAN广域网优化，削减带宽、优化访问体验，降低线路成本和提升访问体验
- 通过SD-WAN智能选路，快速切换业务，保障业务连续性

特性2：云网融合，重构基于云业务WAN网络
解决云网互联面临部署运维复杂、业务连续性差难题

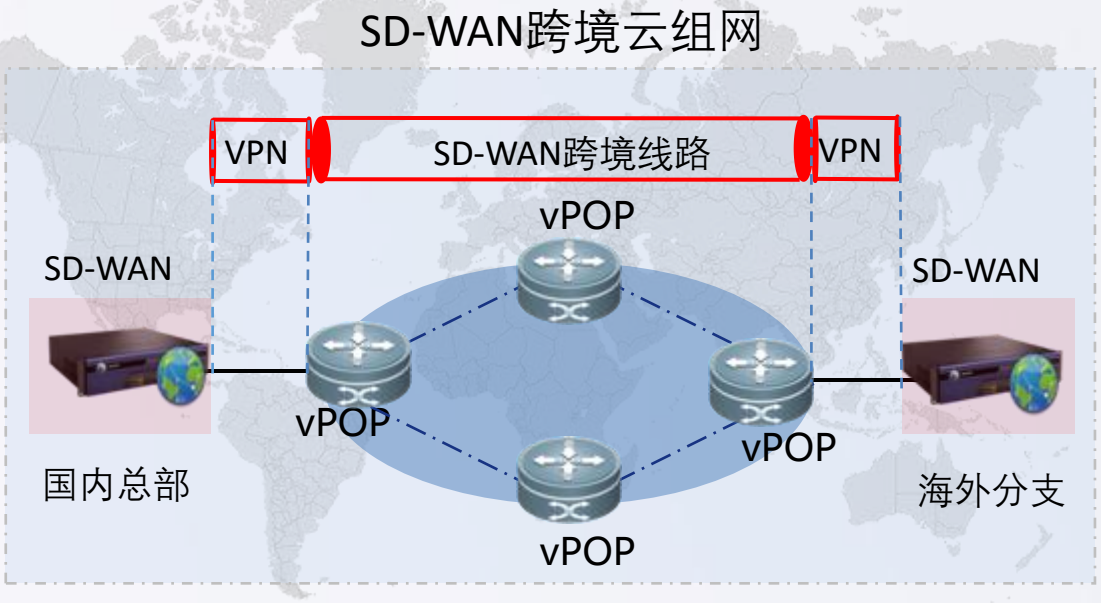


SD-WAN解决云网融合思路:

1、多云互联、分支和云互联，通过SD-WAN快速部署上线、可视化运维管理，实现多分支接入云端或者物理数据中心易部署、易运维。

2、SD-WAN故障秒级切换，保障业务连续性

特性3：跨境组网，基于全球云节点构建高速网络 降低专线成本、提升访问体验



◆降低成本：相比专线方案TCO降低50%

◆提高访问体验：提供网络质量保证，媲美专线质量

SD-WAN为您带来四大业务价值

节省线路费用

解决方案: SD-WAN 避免提高带宽带来的费用飙涨

- MPLS捆绑低费用的链路例如宽带或4G/3G
- 最高节省80%

提高访问体验

解决方案: SD-WAN 通过避免网络问题确保用户体验性

- 通过实时最佳链路选择避免应用性能受影响
- 通过策略保证重要应用的性能

保障业务连续性

解决方案: SD-WAN 提供永续的业务服务

- 通过虚拟捆绑多条WAN链路实现更可靠的连通性
- 通过实时改变应用数据流实现业务永续

运维可视

解决方案: SD-WAN可可视监控设备、应用、网络

- 可视化展示全网分支健康状况;
- VPN拓扑展示链路、VPN应用、应用QOE;
- 安全大屏展现全网安全漏洞。

深信服SD-WAN解决方案框架

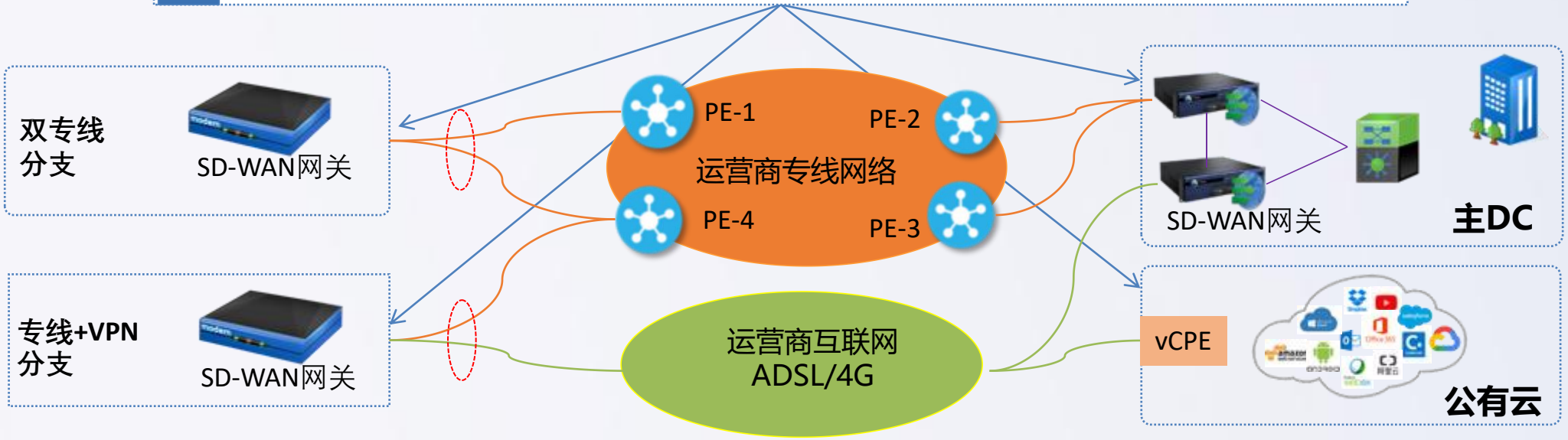
SANGFOR 深信服科技

云集中管理

分支健康状态大图

线路及应用状态可视

安全风险大屏



SD-WAN = **WAN池化和选路** + **WAN优化** + **WAN可视管理** + **WAN安全**

- 建立overlay隧道
- 四大智能选路策略
- 应用优先级编排
- 秒级故障切换

- 应用优化
- 链路优化
- 数据优化
- 视频优化

- 邮件开局易部署
- AUTO VPN自动配置
- 全网可视化运维和监控

- NFV组件按需部署
- 安全组网融合一体
- 上网行为管理
- 边界七层防火墙

深信服SD-WAN核心优势功能

选路

高效智能选路

- 提升带宽利用率至100%
- 故障秒级切换

优化

极致访问体验

- 提升300%访问速度
- 降低40%线路成本

安全

业界领先安全能力

- 分支边界2-7层安全
- 全网态势秒级感知

可视

可视化管理

- 分支分钟级部署
- 链路、应用、安全多维度可视监控

SD-WAN案例：5000+客户应用

SANGFOR 深信服科技

政府

医疗

金融

商业

物流

能源

科技

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

安视交换机

深信服安视交换机产品概述

传统网络亟需解决的问题：（1）海量命令行配置，配置复杂 极易出错；（2）访问趋势 无法洞察；（3）使用操作不规范，终端违规，事件频发。万物互联时代对网络安全提出更高要求，要求交换设备要更安全、业务访问更可视、运维更智能简单

安视交换机创新应用

SANGFOR 深信服科技

连接更安全

- 安全联动实现系统安全
- 实时感知网络终端特征
- 提高网络接入认证安全性

业务更可视

- 网络数据图像化一目了然
- 多视角呈现网络安全实况
- 接入终端识别，资产统一更清晰

运维更简单

- 实现设备零配置上线
- 图形化界面操作更便捷
- 网随人动，不再多次配置

下一代智能交换机特性优势

• 网络自动化

- 二层广播
- 三层IP
- 域名/DNS
- DHCP Option
- 扫码上线
- 全自动化（MAC/SN）

• L2 / L3

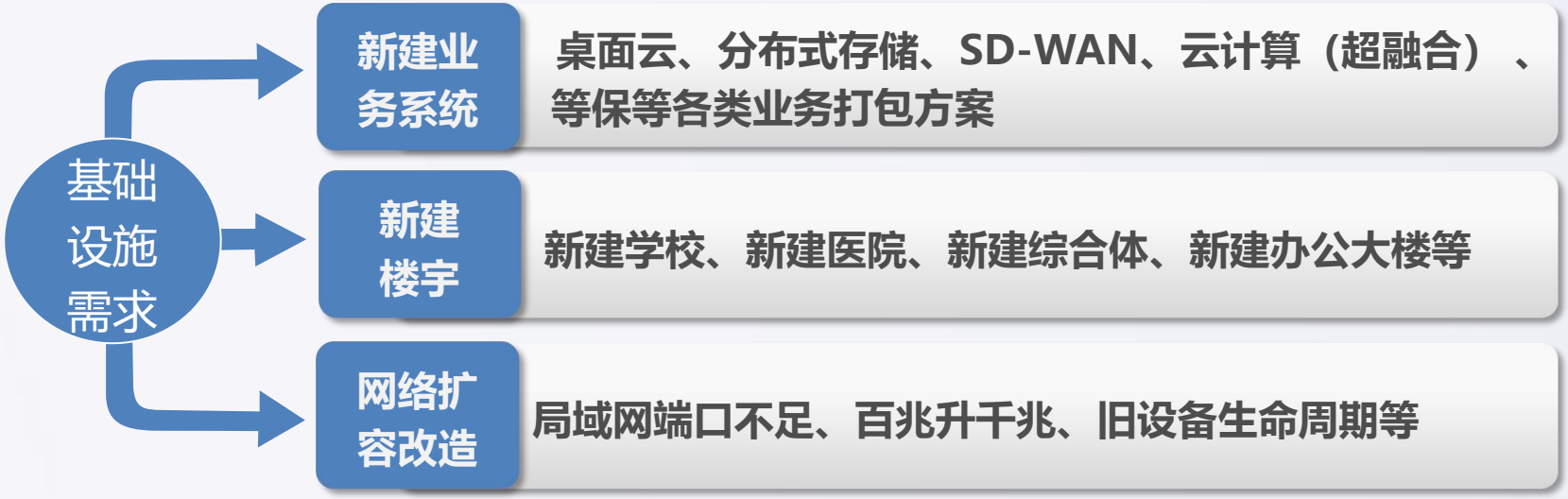
- VLAN
- STP/MSTP/RSTP
- M-LAG虚拟化
- 静态路由/RIP/OSPF
- 端口聚合/流量镜像
- ACL/QoS
- 组播/IGMP Snooping
- DHCP/DHCP Snooping

• SDN（软件定义网络）

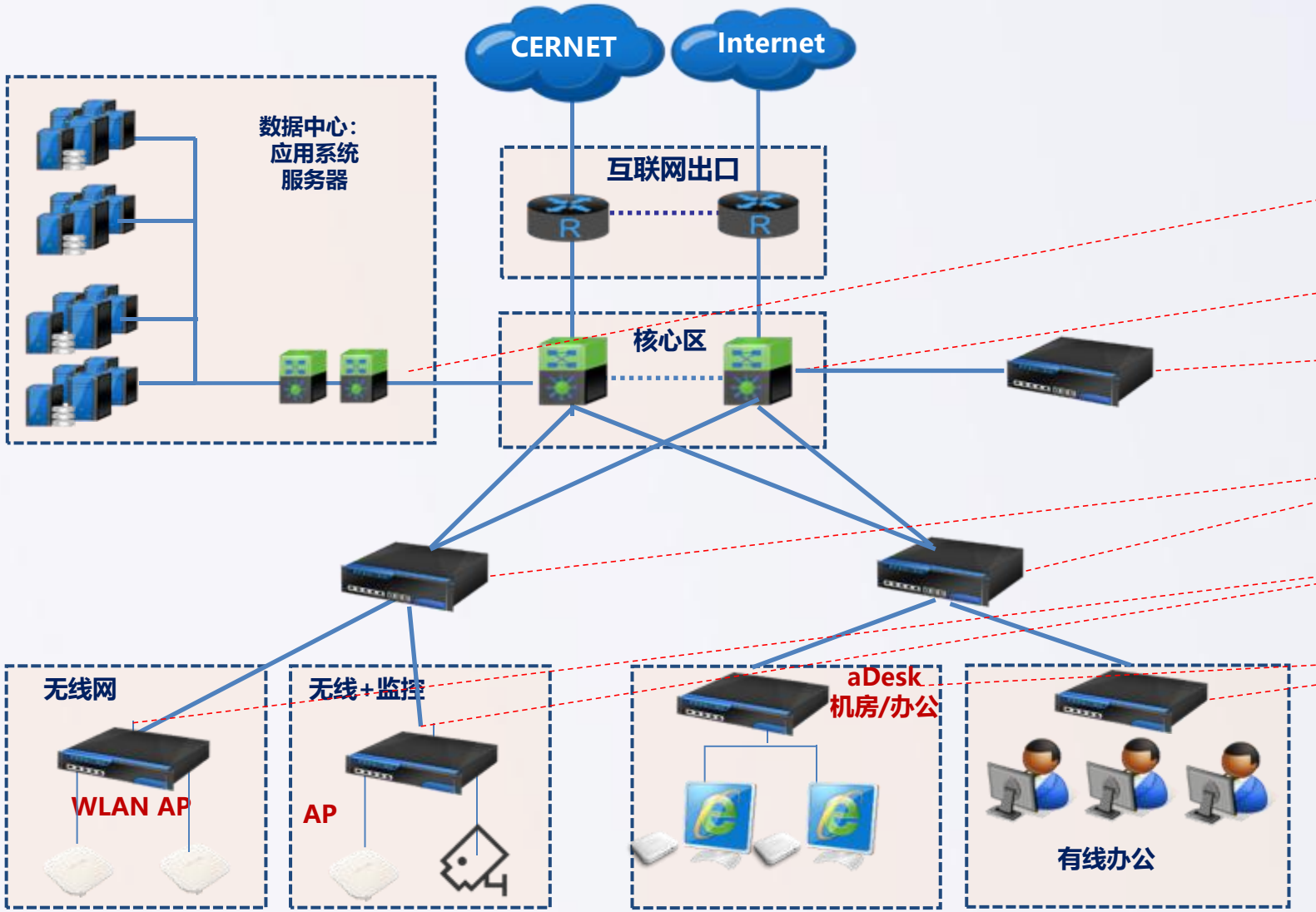
- 零配置上线
- 统一配置管理
- 旧设备一键替换
- 端口终端识别
- 联合安全防火墙
- 网络安全画像

基于软件定义网络新型架构进行全新设计，支持通过控制器对所有交换机进行统一配置管理，相比于传统的管理型交换机，不再需要单独配置，并且支持交换机零配置上线到控制器，所有的管理都是图形可视化操作，避免复杂的CLI命令行配置。

深信服交换机市场的机会点在哪里



交换机的应用场景



数据中心交换机

核心交换机

NAC控制器

汇聚交换机

POE接入交换机

接入交换机

SANGFOR
深信服科技

一. 深信服产品系概述

二. 云端安全产品介绍

三. 网络安全产品介绍

四. 终端系列产品介绍

五. 基础网络产品介绍

六. 数据中心产品介绍

七. 安全合规产品介绍

八. 运营管理产品介绍

九. 产品推广工具介绍

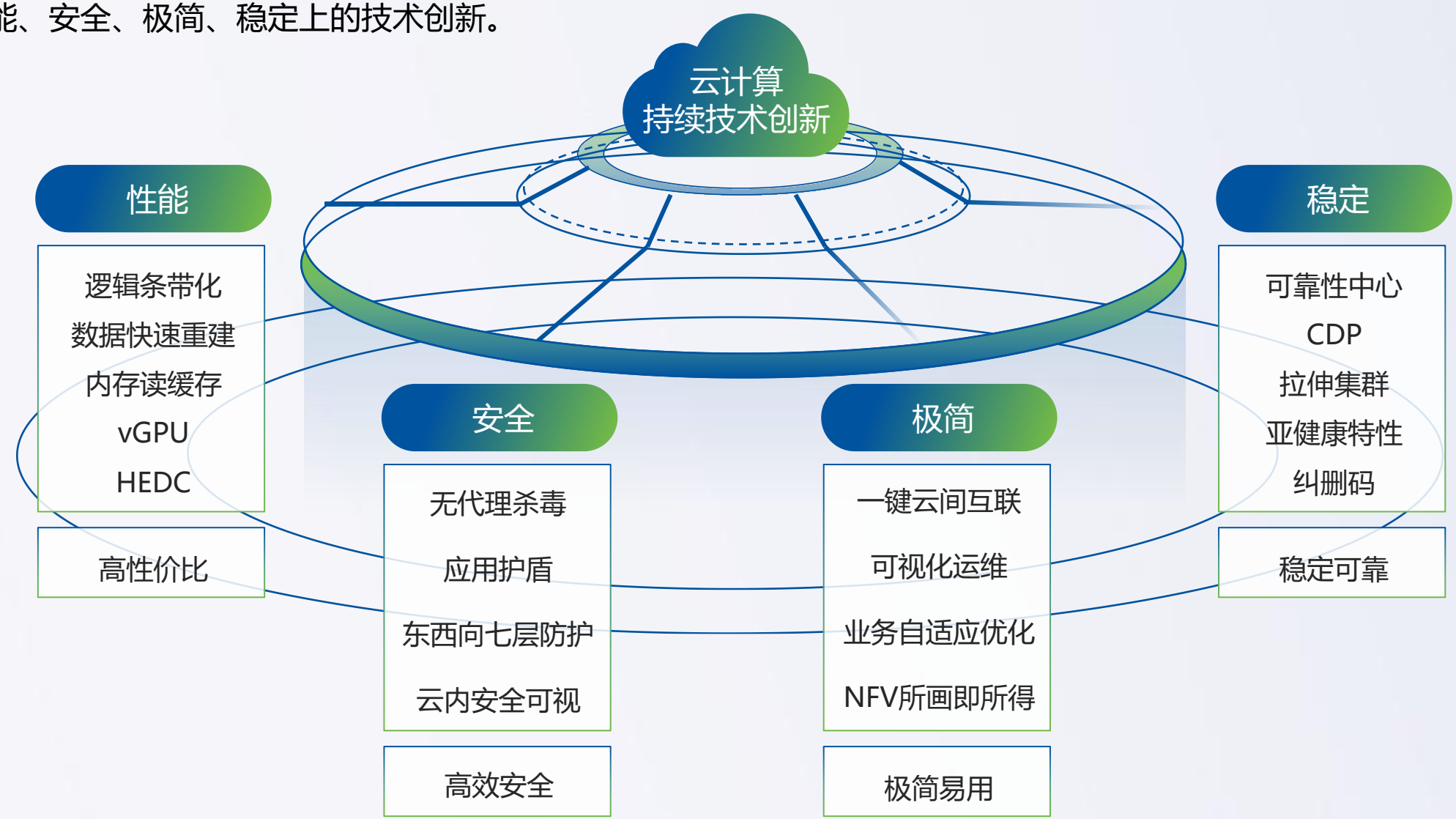
SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

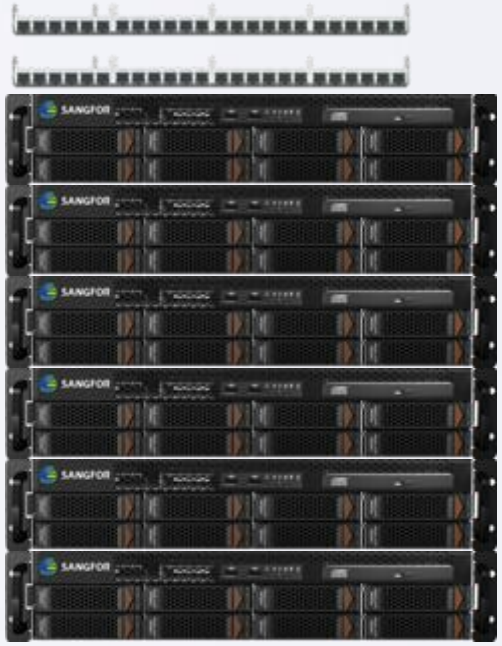
云计算 aCloud

云计算aCloud产品概述

深信服超融合解决方案，通过软件定义，将数据中心里的计算、存储、网络、安全、管理以及大数据等核心基础能力，通过软件化，灌装到标准的服务器里面去，再通过简单的服务器堆叠来构建超融合架构的云计算解决方案。这样的解决方案带来性能、安全、极简、稳定上的技术创新。



深信服创新“极简架构”超融合aCloud



超融合架构
的云计算方案

1
特点

极简：2种物理设备，满足传统5类IT基础需求

- 替代人员机房运维操作
  - 多租户、编排、运维、审批...
- 替代硬件网络安全设备
  - vIAM 、vAF、vAD、vVPN...
- 替代硬件二三层交换机高级功能
  - aSwitch、aRoutor、aFW
- 替代外置中低端存储
  - aSAN 、aStor
- 替代服务器
  - KVM、Docker、vGPU

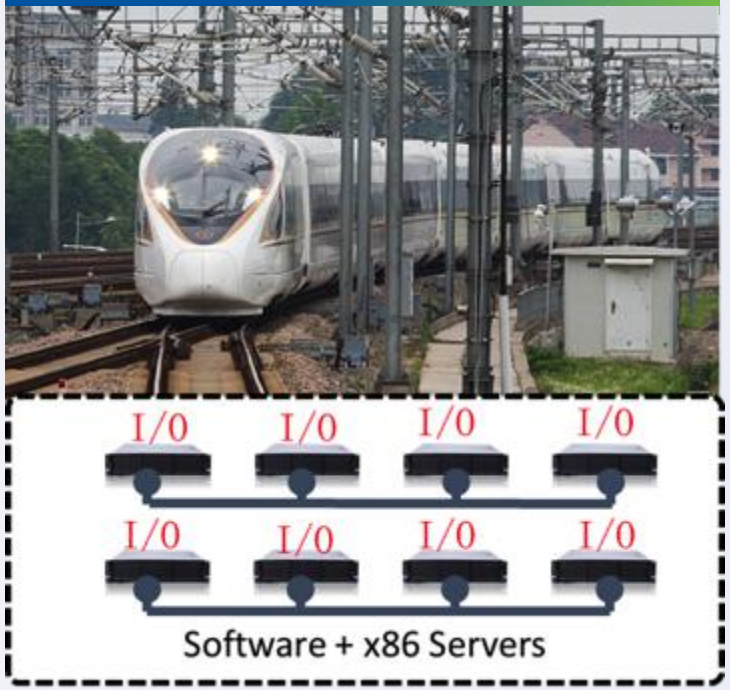
2
特点

稳定：分布式和多副本机制降低数据计算风险

传统架构

VS

分布式架构



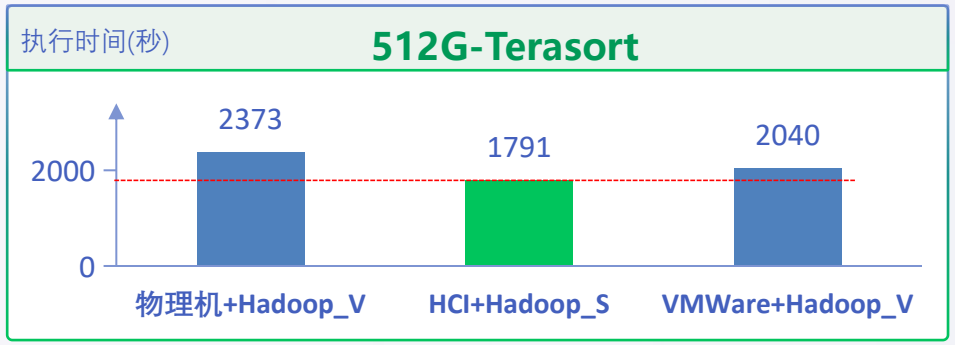
- 软件定义分布式存储 scale-out 扩容，每个节点都提供I/O：容量扩展、性能扩展
- 分布式故障恢复快，6主机集群重建速度可达**1TB/30min**
- 加/减硬件时数据自动迁移，无需人工干预

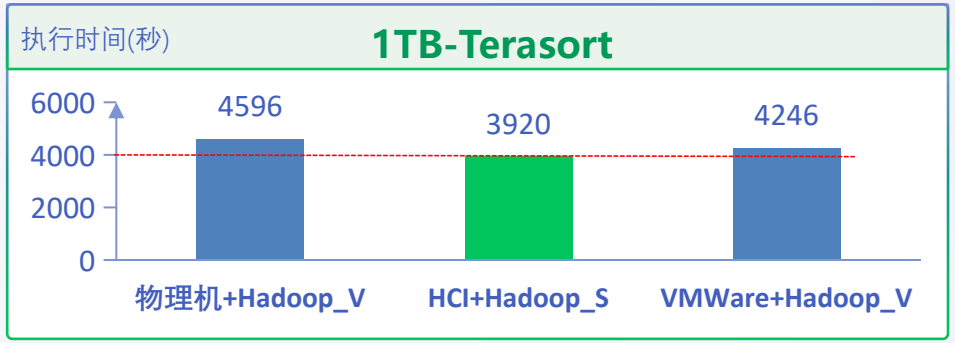
3
特点

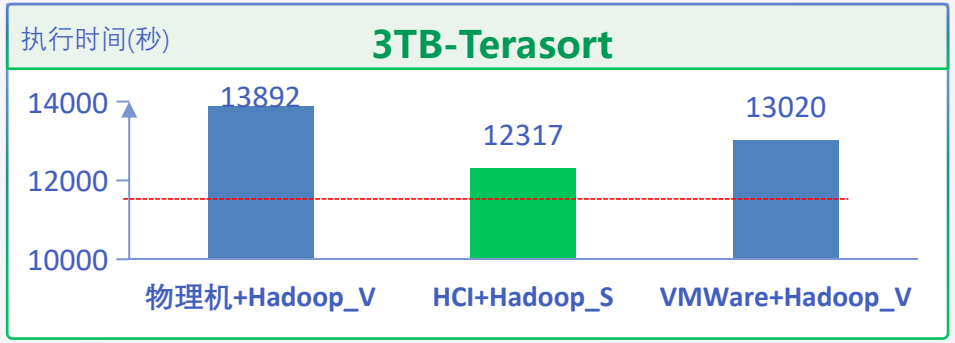
高性能：满足大数据场景高速计算性能需求

3
特点

高性能：大数据场景对比VMware性能提升7%







CPU	32核，Intel® Xeon® CPU E5-2630 v3® 2.4Hz
内存	128GB
HCI版本	aCloud 5.8.5
VMware版本	Esxi6.7版本
Hadoop版本	Hadoop 2.6.5
Linux内核版本	Linux version 3.10.0
Benchmark	Terasort(CPU、内存和I/O操作密集型的程序)
数据来源	TeraGen产生

比VMware性能提升：

平均：**7.3%↑**　　最好：**10%**

* Hadoop_V：VMware最佳实践配置
* Hadoop_S：深信服智能配置

围绕极简、稳定、高性能设计了四大解决方案

1

承载关键业务
解决方案

2

超融合云数据中心
解决方案

数据中心容灾备份
解决方案

3

涉密虚拟化
解决方案

4

SANGFOR 深信服科技

政府客户的广泛认可

企业客户的广泛认可

大族激光 HAN'S LASER

- 提升ERP、数据库等核心业务的可靠性
- 财务系统月底报表生成从20小时缩短到8小时

教育客户的广泛认可

武汉大学 WUHAN UNIVERSITY

- 140台服务器，全校所有业务上云
- 超融合一体机集群替换1000万Oracle数据库一体机
- 保障开学1.8万新生入学、迎新和选课系统高效运转

西南大学 SOUTHWEST UNIVERSITY
中国矿业大学 CHINA UNIVERSITY OF MINING AND TECHNOLOGY
中国地质大学 CHINA UNIVERSITY OF GEOSCIENCES
宁夏师范学院 NINGXIA NORMAL UNIVERSITY
中南大学 CENTRAL SOUTH UNIVERSITY
河南大学 HENAN UNIVERSITY
南方科技大学 SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY
浙江大学宁波理工学院 Ningbo Institute of Technology, Zhejiang University
海南大学 HAINAN UNIVERSITY
荆州职业技术学院 JINGZHOU INSTITUTE OF TECHNOLOGY
湖南文理学院 Hunan University of Arts and Science
沈阳建筑大学 SHENYANG JIANZHU UNIVERSITY
河南科技学院 Henan Institute of Science and Technology
深圳大学 SHENZHEN UNIVERSITY
青海卫生职业技术学院 QINGHAI INSTITUTE OF HEALTH SCIENCES
山东信息职业技术学院
福建省上杭职业中专学校 http://www.shzyzz.com
深圳信息职业技术学院 SHENZHEN INSTITUTE OF INFORMATION TECHNOLOGY
江西财经职业学院 Jiangxi Vocational College of Finance and Economics
扬州市汶河小学 YANGZHOU WENHE PRIMARY SCHOOL
北京电子信息技师学院

金融客户的广泛认可

海通期货 HAITONG FUTURES

- 100台服务器减少到27台，每年节省租凭费用100万
- 部署开发环境、测试环境，从1天到30分钟

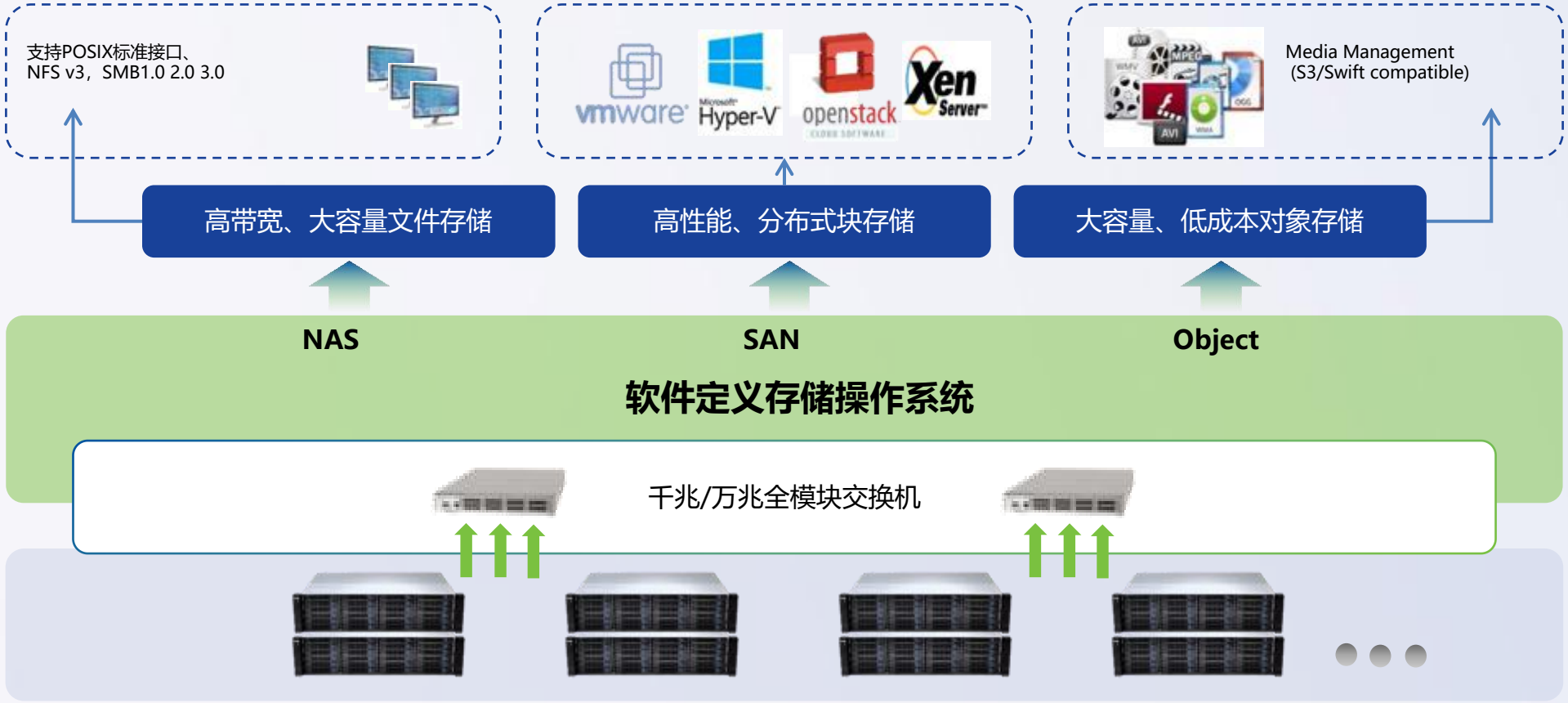
SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

企业级分布式存储EDS

企业级分布式存储EDS产品概述

传统存储在性能、扩展性、管理、数据孤岛等多种问题，通过一个智能云存储平台来解决这些难度，首先统一平台，主要从两方面，一个是智能，这是存储未来的一个新能力，会更多植入AI技术和模型，将过去传统存储只是单纯做数据存放，转变为可以实现智能的数据管理，也就是不仅要做好数据存放，还要做好智能优化、智能运维和价值评估等工作；另一个是云化，要将存储变成资源池的方式，提供多种类型的存储方案，包括对象、文件和块等，满足前端各种业务需求。



统一平台，融合所有存储服务及应用，创造数据“新”价值

深信服“软硬件一体化”分布式存储EDS

企业级分布式存储EDS

集群部署，可实现千万级IOPS及数百GB/s吞吐性能

软硬件一体化交付

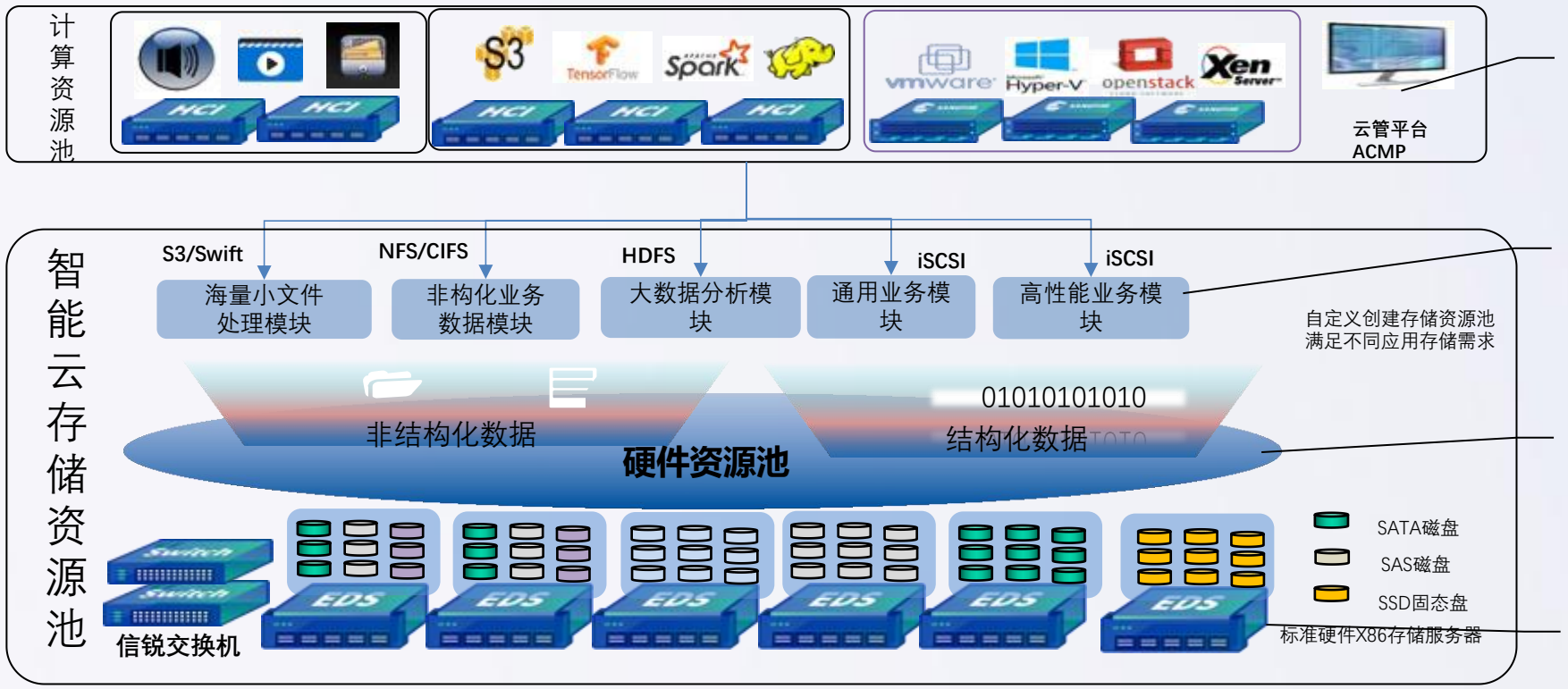
EDS1210/1250

EDS3600

EDS存储一体机

型号	EDS1210	EDS1250	EDS3600
定位	小容量非结构化数据存储	高性能块存储	大容量数据存储
数据盘	12个盘位	12个盘位	36个盘位
存储接口类型	iSCSI、NFS、CIFS、HDFS、S3		
最大节点数量	5000个		
最大存储容量	EB级		

深信服EDS存储平台拓扑图



深信服aCmp云管或兼容第三方云管平台

自定义逻辑分区，根据业务系统需求自定义创建，满足多类型存储需求。

由EDS分布式系统构建统一存储资源池，可同时提供块、文件、对象及HDFS多种存储接口，满足多种业务需求。

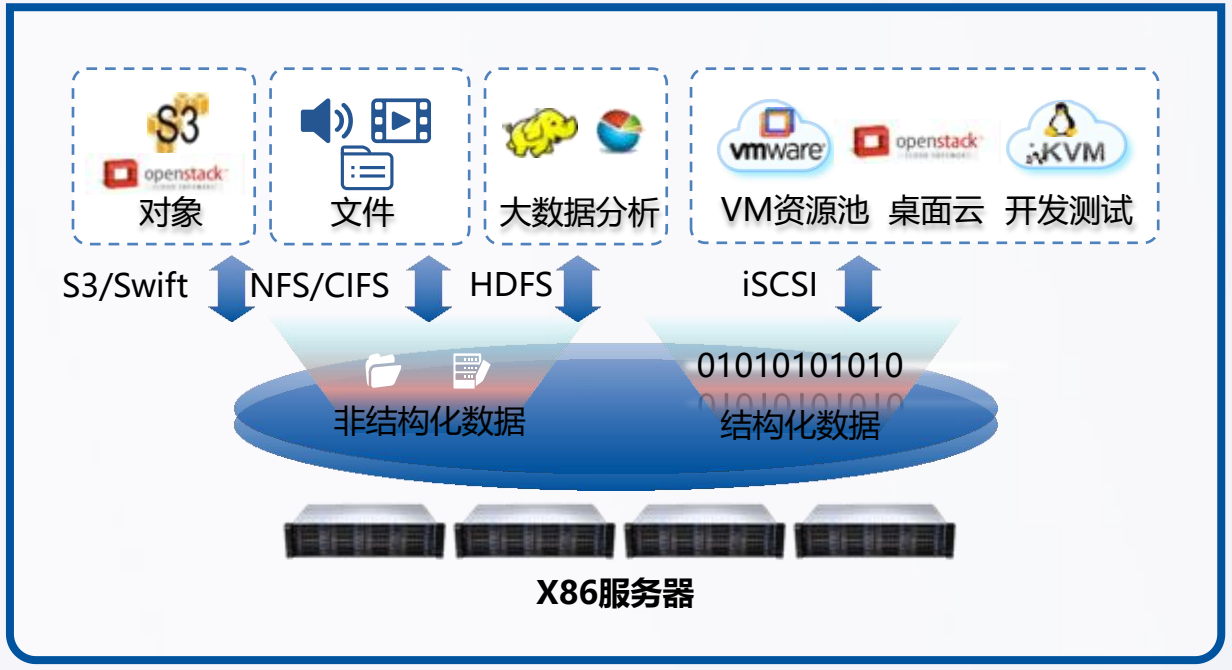
EDS存储一体机/标准企业级服务器

统一平台，融合所有数据存储服务及应用，创数据新价值

应用场景一：数据中心云存储

SANGFOR 深信服科技

全面兼容KVM、ESXi、XEN、Hyper-V、OpenStack、华为、华三等

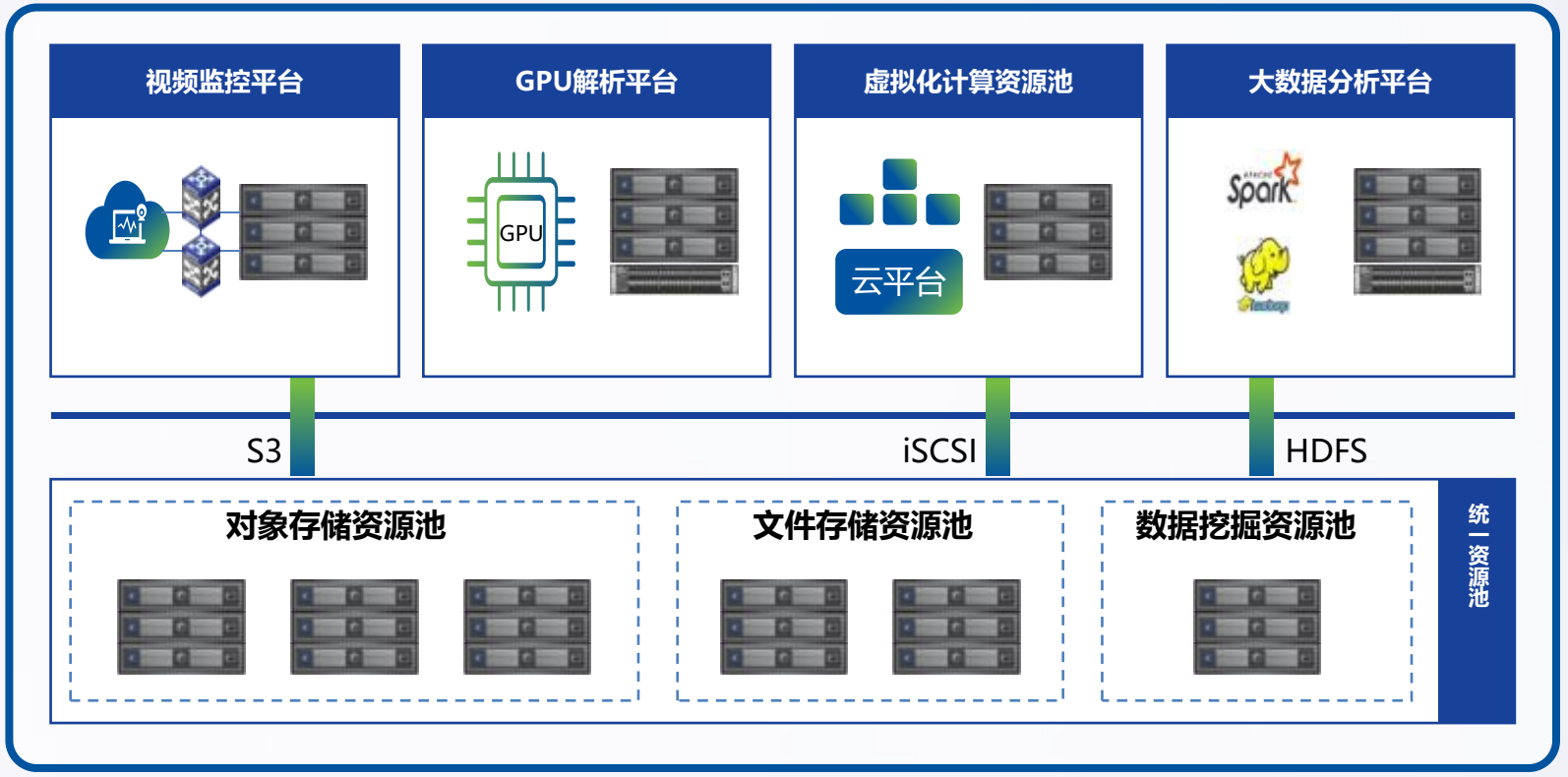


- **超高性能支撑多元化业务**
- **超高可靠性保障业务可用**
- **统一存储满足多样化需求**

应用场景二：海量非结构化数据存储

SANGFOR 深信服科技

适用于海量小文件存储、EB级大容量存储、高性能计算等场景（广电媒资、能源勘探、卫星测绘、政府监控、人脸识别、金融影像平台等多种行业）



- **5000节点EB级容量扩展**
- **百亿级小文件高性能处理**
- **海量小文件高效秒级检索**

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

应用交付AD

应用交付AD产品概述

深信服应用交付（AD）解决方案是对应用数据进行端到端的分析、调度、保护、加密和优化，集服务器负载、链路负载、全局负载和SSL卸载等于一体，能够探测应用交付过程中的故障，并毫秒级切换，保障应用稳定。

链路负载均衡、服务器负载、全局负载均衡All In One，三种功能同时处于激活可使用状态，无需额外购买相应授权。

基础：
多链路负载均衡
服务器负载均衡
多数据中心负载均衡
SSL卸载

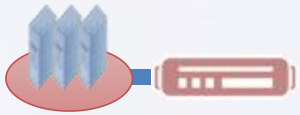
延伸：
服务器性能优化（如SSL卸载、HTTP压缩、TCP链接复用）
单边加速、图片转码
虚拟化（VAD+AD软件版）

深信服应用交付：应用场景

场景一

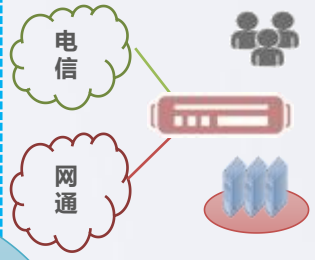
数据中心-保障应用系统可靠性和高性能

- 业务多服务器负载
- 系统健康监控
- 卸载服务器压力
- 业务加速
- 系统安全防护



场景二

互联网出口-多链路出入站智能选路



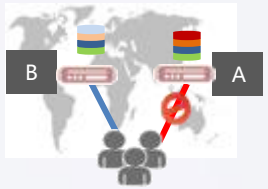
- 多条链路流量分担
- 链路健康监控
- 智能DNS代理

四大应用场景

场景三

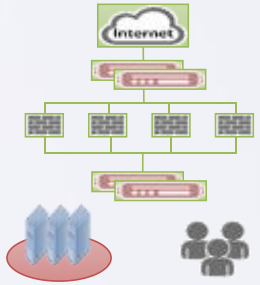
双活数据中心，灾备中心负载均衡

- 内置智能DNS服务器
- 根据地域，运营商，数据中心资源利用率分配流量
- 数据中心健康监控



场景四

安全/应用设备负载



- 异构设备实现集群
- 提高扩展能力
- 解放安全设备自身开启集群的性能占用，提高处理能力

SSL安全网关国密产品

国密算法支持

针对国密SM算法支持，有效规避公共安全漏洞；
同一个站点（虚拟服务）同时支持国密和RSA证书，保障业务向国密算法平滑扩展。

认证全面性

支持单向/双向SSL证书认证；
支持RSA1024bit/2048bit秘钥长度；
支持国密SM2的256bit证书秘钥长度。

更强适用性

支持不同的证书信息透传编码格式；
支持向后台服务器传递证书和证书指定参数；
允许客户端证书最小秘钥长度的设置。

全面服务器负载策略

全面四、七层负载均衡算法；
多种会话保持方式；
针对服务器和业务主动+被动监控检查。

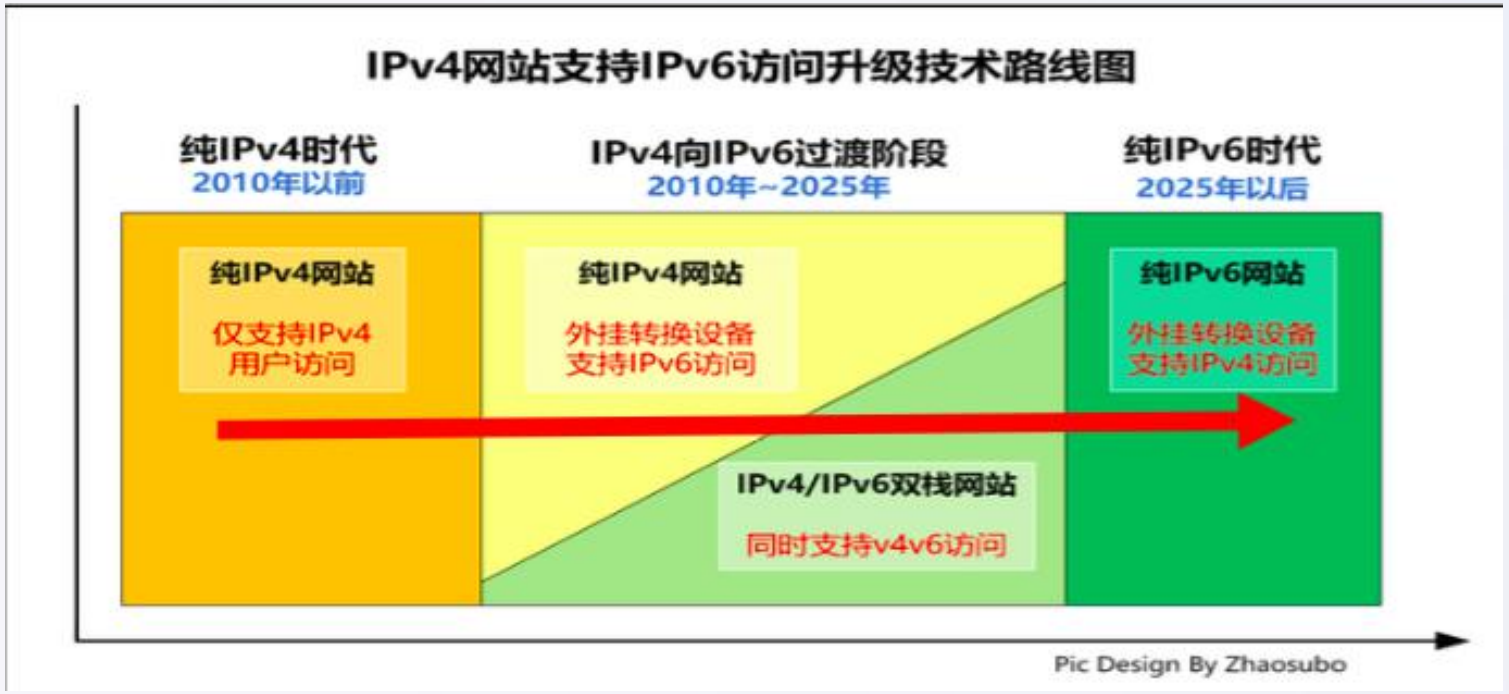
IPv6解决方案

1、IPv4/IPv6 双栈是最为彻底的一种网站支持IPv6 升级改造技术，概念清晰，易于理解，升级工作一步到位，永久解决问题。是 互联网向 IPv6 演进升级的最终目标。

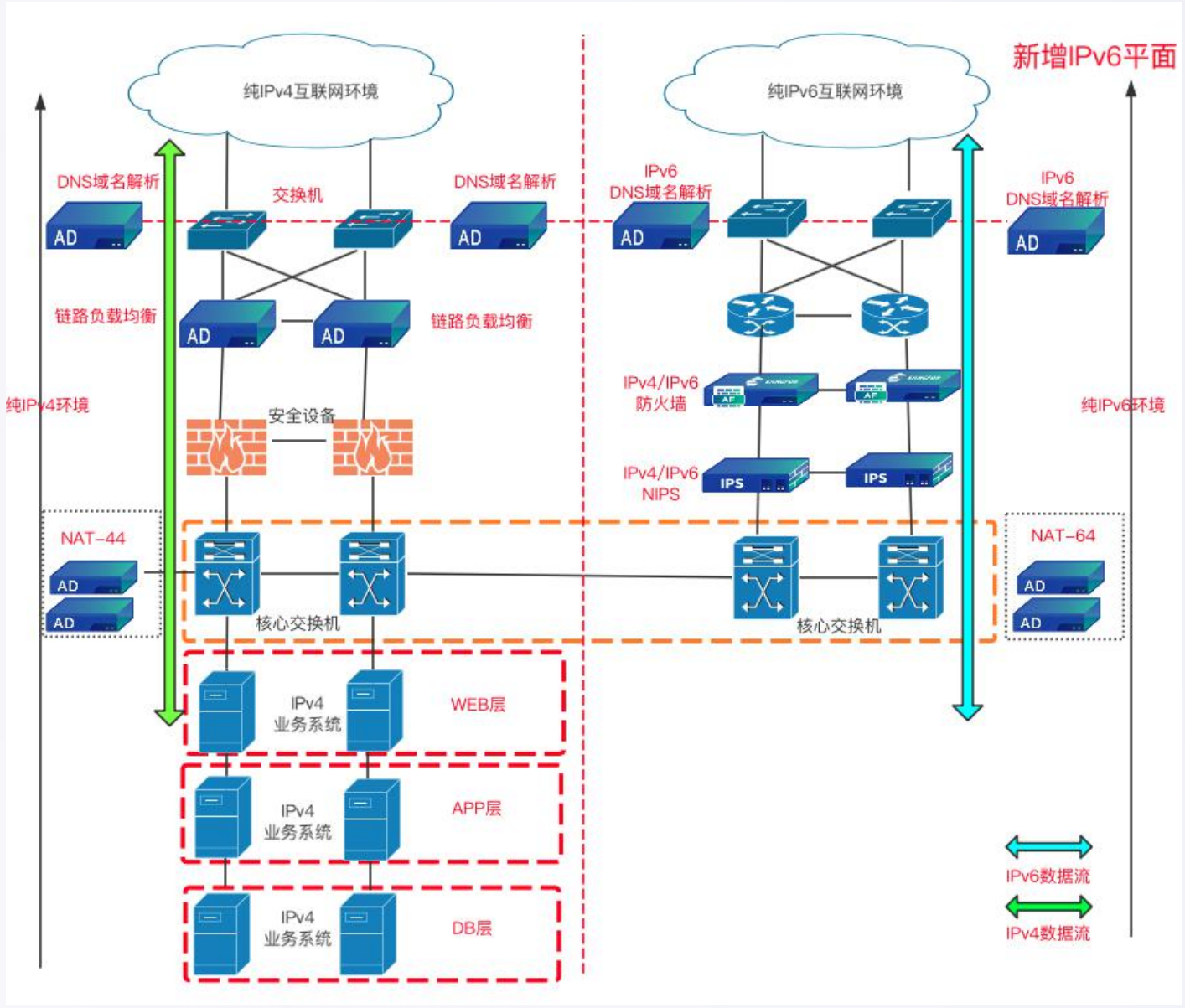
2、同时运行 IPv4 和 IPv6 两个协议栈，可实 现IPv4对IPv4、IPv6对IPv6的单协议栈通信，访问效果较好。

3、国家要求从2018年起，新建政府网站和应用系统必须支持IPv6，新建网站和应用系统应直接采用双栈。

4、网站改造，新建不久的网站、结构不太复杂 的网站，适用于从IPv4改造为双栈。



IPv6改造解决方案—新增平面转换1



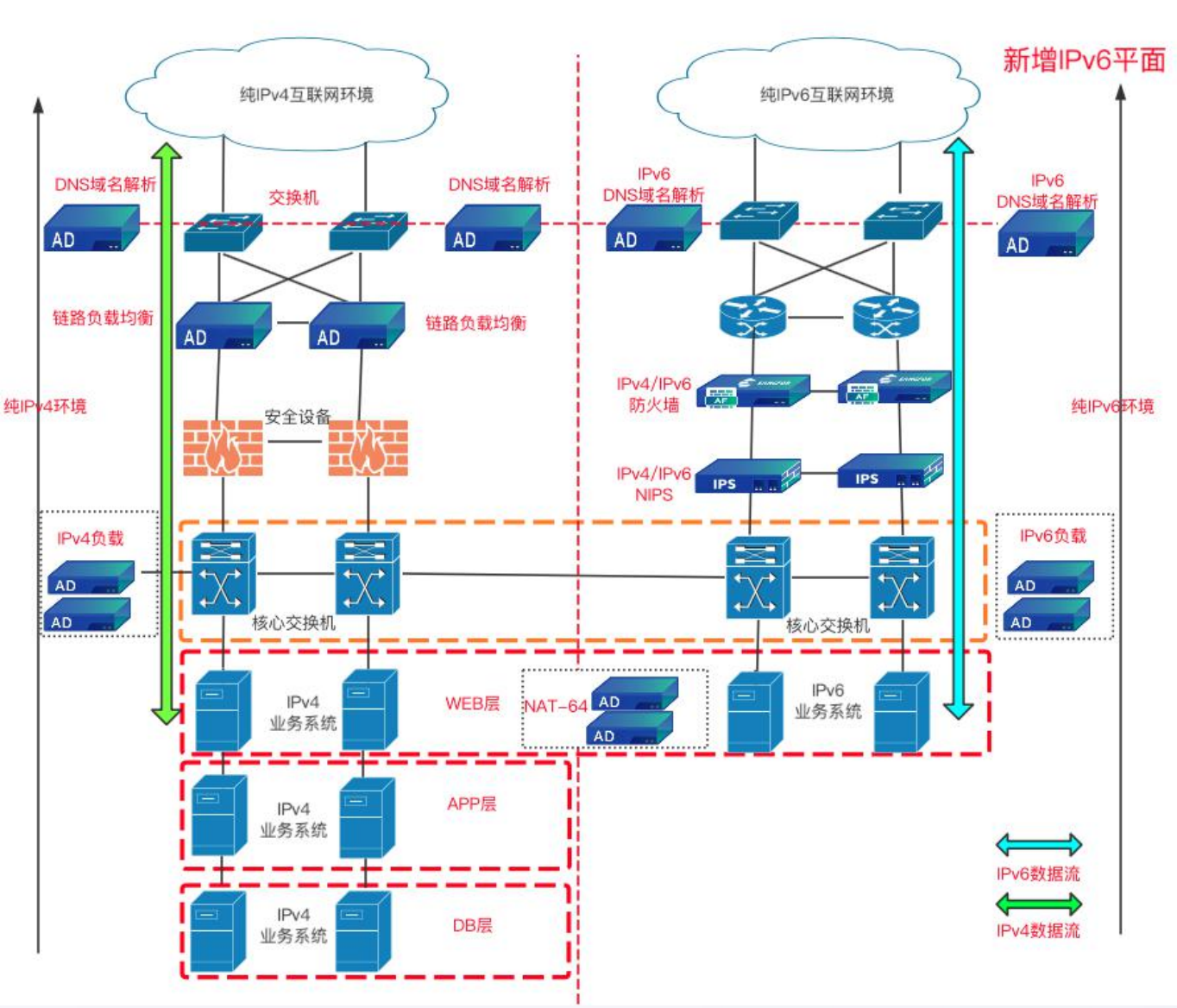
方案说明：

- 运营商分别提供IPv4、IPv6接入，保持原有IPv4内网网络和应用不变
- 新增IPv6转换设备接入后端复用IPv4现有的应用系统。
- 新增平面增加网络安全设备、DNS设备和IPv6转换设备

方案特点：

- 对目前已有IPv4网络和应用无任何改动；
- 面向公众业务重要且访问量大，通过新增平面避免同一设备同时承载IPv4流量和IPv6流量造成的性能瓶颈问题（IPv6损耗大）；
- 不用对现有的应用进行改造，改造难度低，易于快速完成。
- IPv4和IPv6分流，做到故障隔离，便于出现问题及时排查。
- 通过部署安全设备对IPv6网络进行防护，满足监管发文中IPv6改造后安全防护程度不低于现有IPv4防护程度的要求。

IPv6改造解决方案—新增平面转换2



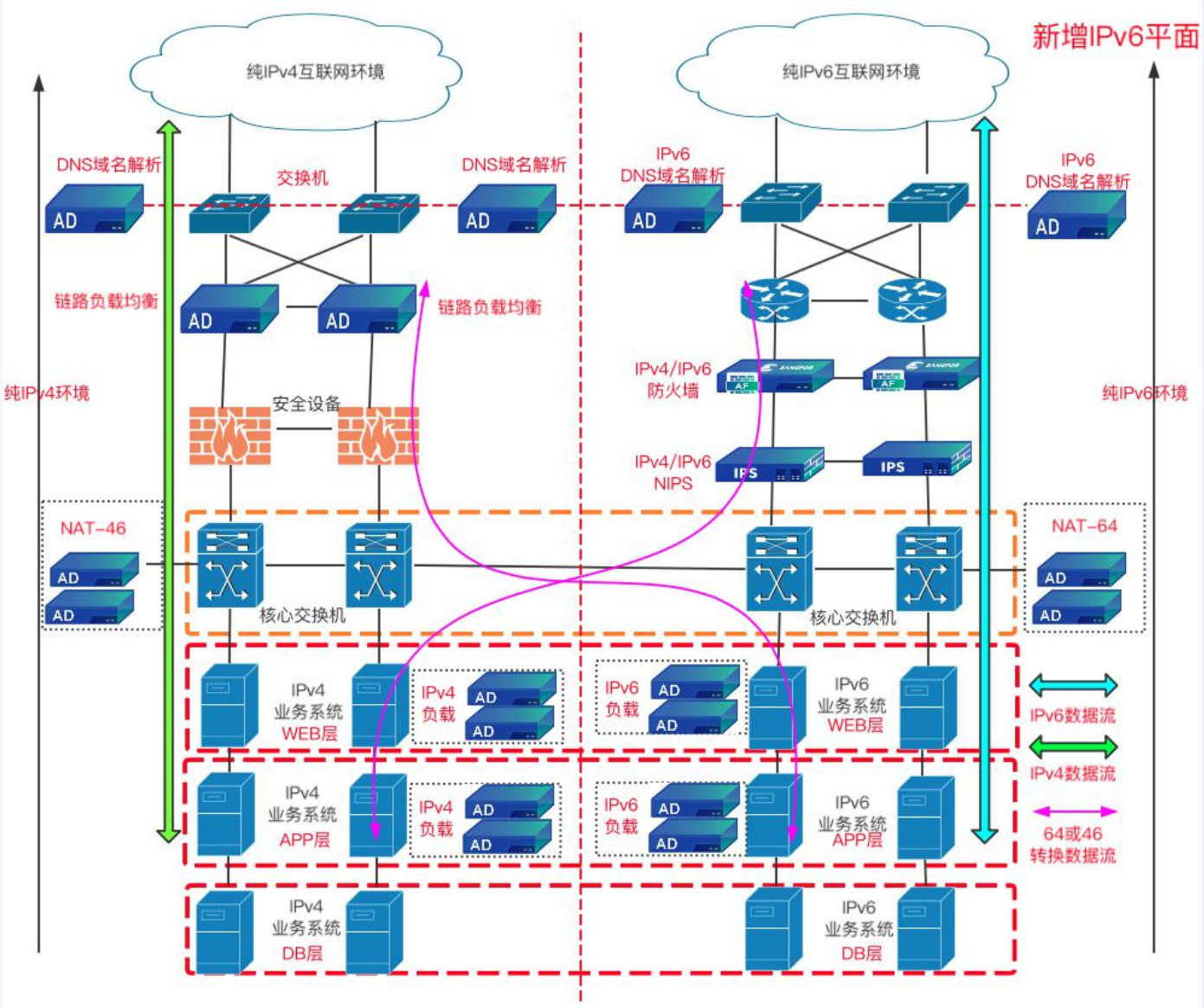
方案说明：

- 运营商分别提供IPv4、IPv6接入，保持原有IPv4内网网络和应用不变
- 新增IPv6负载设备对WEB层IPv6应用进行服务器负载
- 新增IPv6转换设备接入后端复用IPv4现有APP层以下的应用系统，WEB层系统进行IPv6升级。
- 新增平面增加网络安全设备、DNS设备和IPv6转换设备

方案特点：

- 对目前已有IPv4网络和应用无任何改动；
- 面向公众业务重要且访问量大，通过新增平面避免同一设备同时承载IPv4流量和IPv6流量造成的性能瓶颈问题（IPv6损耗大）；
- 对WEB层进行改造，难度相对适中，同时为后续业务系统升级IPv6积累经验（针对有一定技术能力的金融客户）
- IPv4和IPv6分流，做到故障隔离，便于出现问题及时排查。
- 通过部署安全设备对IPv6网络进行防护，满足监管发文中IPv6改造后安全防护程度不低于现有IPv4防护程度的要求。

网络边界改造-新增平面



方案说明：

- 运营商分别提供IPv4、IPv6接入，保持两个不同的流量平面
- 新增IPv6负载设备分别对WEB层和AAP层IPv6应用进行服务器负载
- 新增IPv6转换设备接入后端复用IPv4现有的应用系统（极少的访问情况）
- 新增平面增加网络安全设备、DNS设备和IPv6转换设备

方案特点：

- 对目前已有IPv4网络和应用无任何改动；
- 面向公众业务重要且访问量大，通过新增平面避免同一设备同时承载IPv4流量和IPv6流量造成的性能瓶颈问题（IPv6损耗大）；
- 部分业务三层均进行改造，难度较大，一般是头部大行或证券等有很强技术能力的客户（如工行、交行等0）
- IPv4和IPv6分流，做到故障隔离，便于出现问题及时排查。
- 通过部署安全设备对IPv6网络进行防护，满足监管发文中IPv6改造后安全防护程度不低于现有IPv4防护程度的要求。

AD成功案例表

政府	金融	运营商	能源电力	大企业	教育科研
最高人民法院	四川银联	陕西移动	国家电网	国美电器	中国科学院计算机网络信息中心
海关总署	北京黄金交易中心	西藏移动	海南电网	招商局集团	邮电工业标准化研究院
环境保护部	河北邮储银行	温州移动	郑煤集团	联想移动	中国建筑西南设计研究院
国土资源部	广西农信社	宁波移动	霍州煤电集团	中航国际	军事医学科学院
国税总局	郑州银行	益阳移动	华能水电	中国铝业公司	长春理工大学
国家气象局	长沙银行	湖北联通	华润电力	长虹集团	重庆邮电大学
国家统计局	爱建证券	甘肃联通	五陵电力	红豆集团	华中农业大学
中国民用航空局	华林证券	黑龙江省联通	华润燃气	雅戈尔集团	广东白云学院
共青团中央	西部证券	河北广电	西部矿业	中青旅遨游网	云南艺术学院
北京市公安局	安诚财产保险	江阴广电	普天海油	宏图三胞	北大附中
山西省财政厅	中融国际信托	陕西电信	大唐先一科技	万科集团	贵阳市电化教育馆

SANGFOR
深信服科技

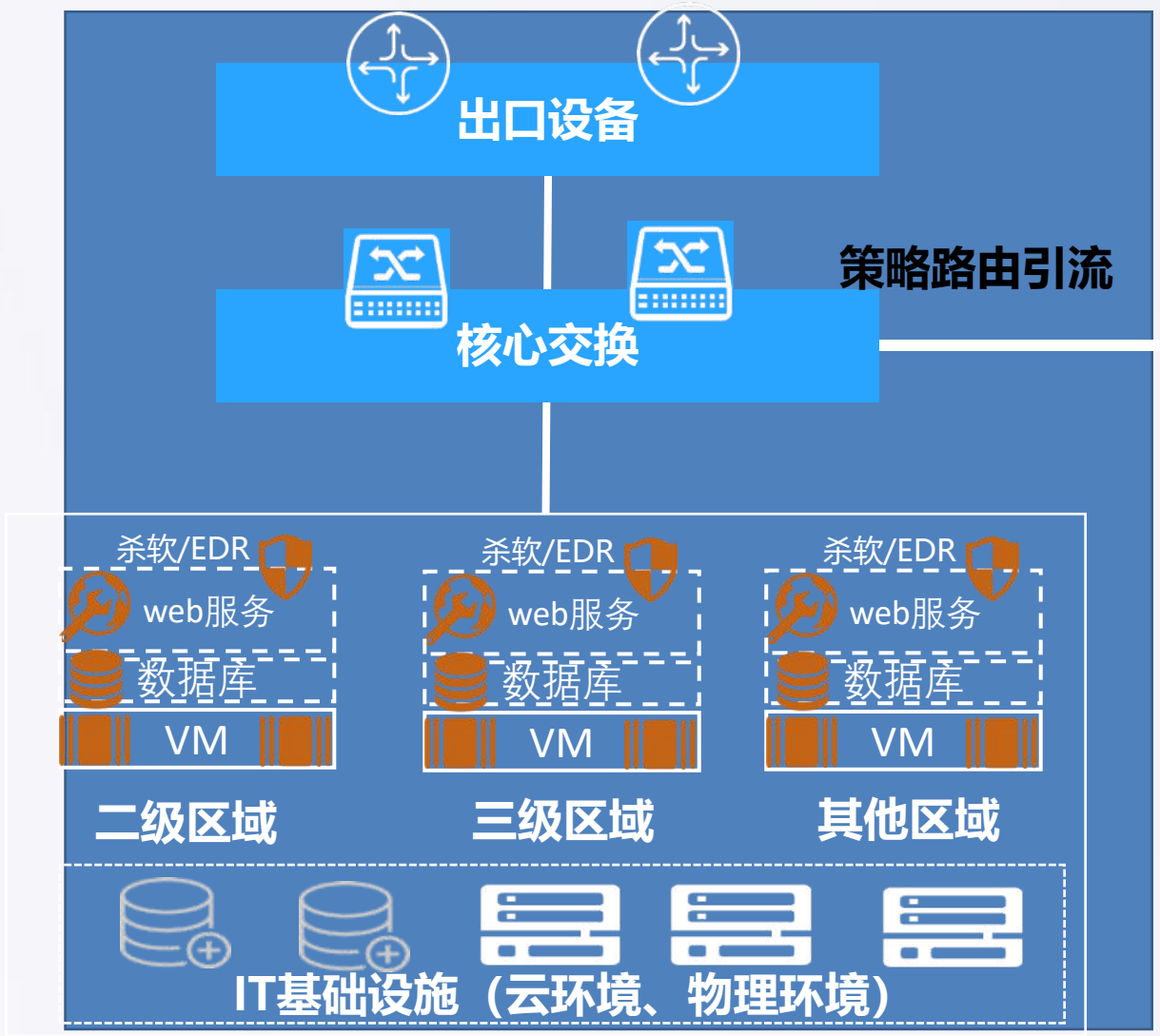
SANGFOR 深信服科技

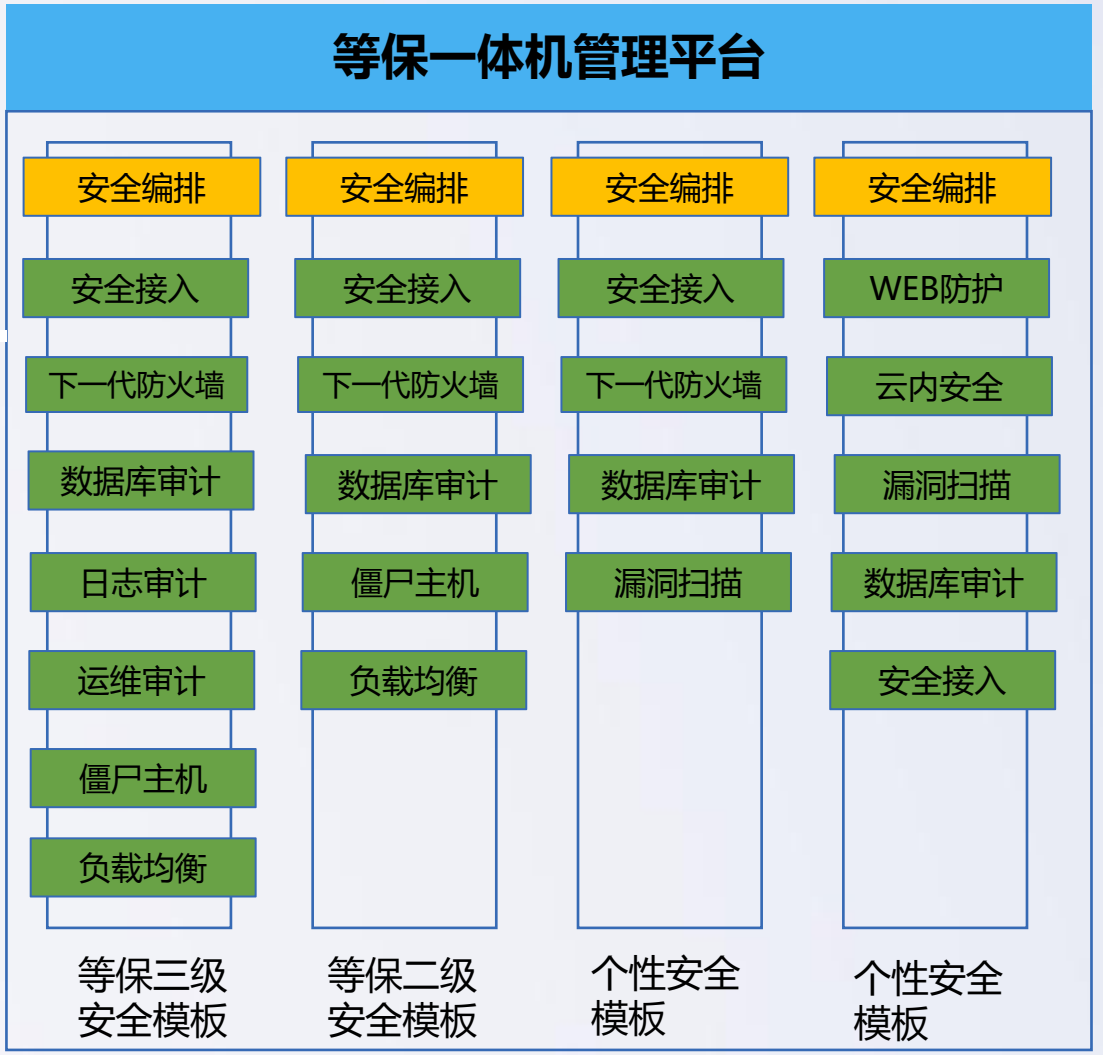
深信服智安全 SANGFOR SECURITY

深信服等保一体机

产品概述

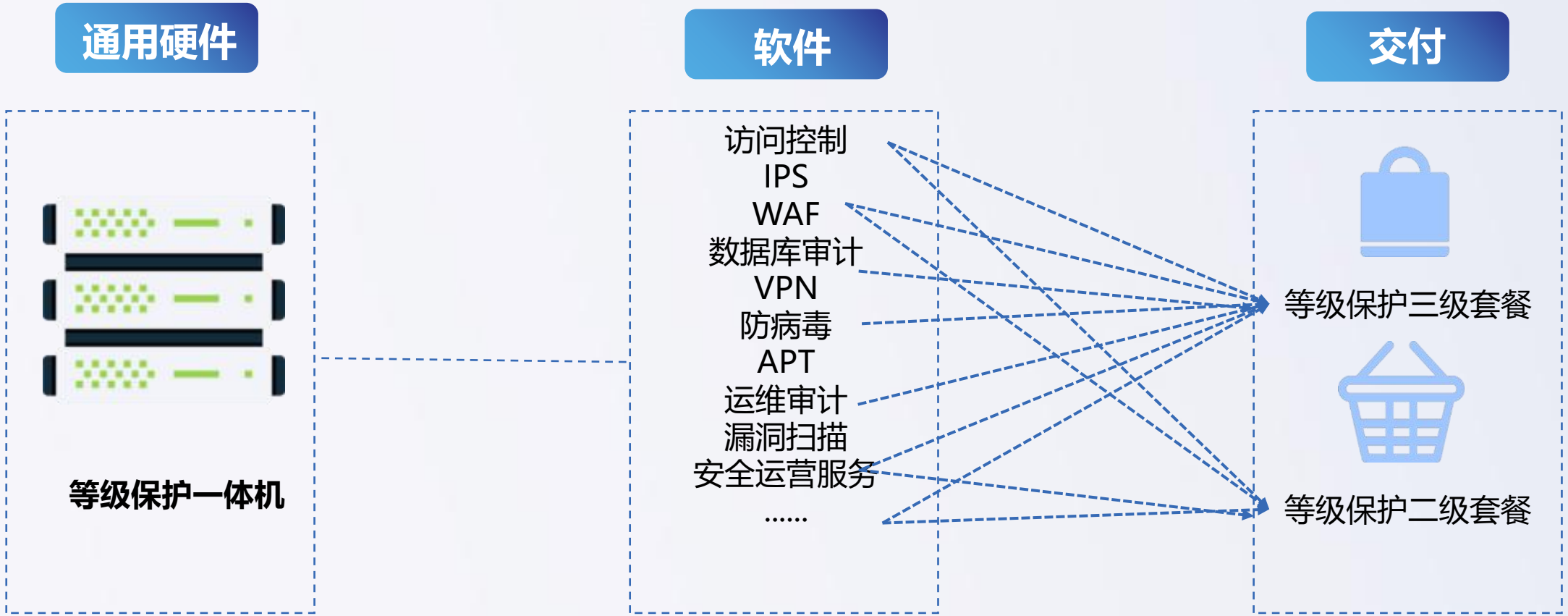
等保一体机解决方案是深信服推出的轻量级、快速交付的一站式解决方案，不仅能够帮助用户快速有效地完成等级保护的建设，同时方案丰富的安全能力，可助力用户为各项业务按需提供个性化的安全增值服务。





产品优势①：支持一站式交付

面向等保合规的一体化、服务化的一站式解决方案



产品优势①：支持一站式交付

面向安全场景的一体化、服务化的一站式解决方案

硬件设备堆叠

安全资源化交付

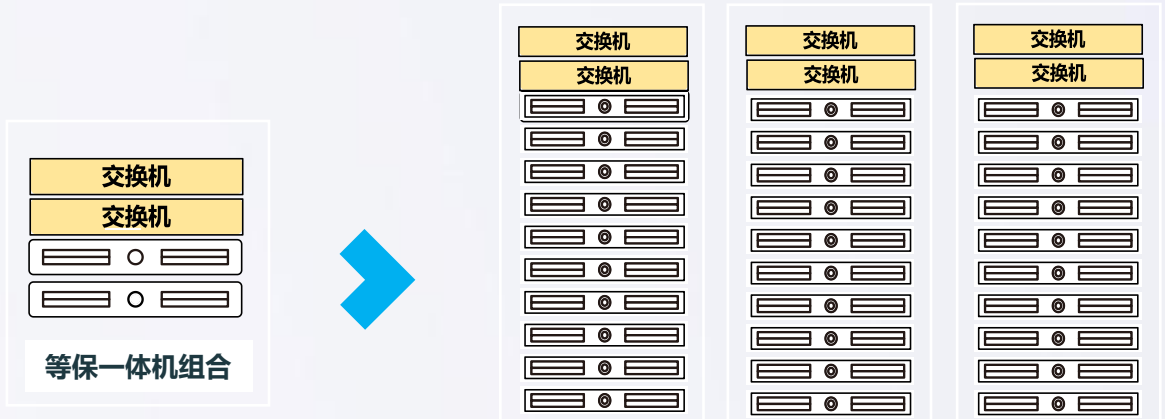
- 下一代防火墙
- 安全接入
- 数据库审计
- ……

安全场景化交付

- 等级保护二、三级场景
- 勒索病毒场景
- 东西向安全隔离场景
- ……

安全功能组件可统一管理，统一下发安全策略

产品优势②：基于软件定义的安全架构，弹性扩展随需而变



按需定义　随需而变　交付简单

- 硬件设备堆叠，建设复杂，周期长
- 设备割裂，运维管理复杂
- 架构固化，难以应对业务环境和政策变化

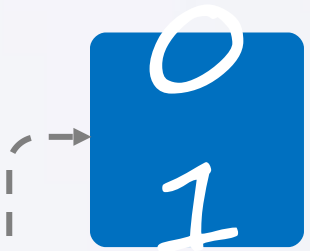
- 软件定义，快速交付
- 安全功能统一管理，减少硬件运维工作
- 组件化安全功能交付，弹性扩展，随需而变

产品优势③：支持网关模式部署

等保一体机支持网关模式部署

通过等保一体机可提供各类安全组件，同时大大简化安全架构

客户价值



安全能力丰富，满足合规要求

深信服等保一体机解决方案涵盖了用户等保建设整改过程中所有技术方面，实现南北向和云平台的东西向安全防护，满足最新等级保护标准要求。

客户价值

降低管理成本与交付周期

传统等保方案需要在网络中部署大量的安全设备，需要大量修改现有网络的结构，深信服等保一体机支持网关模式和旁路引流模式部署，其中旁路引流模式不改变现有网络架构，部署更简单，广泛使用于物理环境和虚拟化环境下的等保建设。

灵活部署，快速交付

传统等保建设需要采购大量的安全设备，深信服等保一体机解决方案用户只需要通过标准的X86服务器搭配上深信服安全资源系统，即可实现传统安全设备实现的所有安全功能，建设成本与交付周期更低。

部分成功案例

SANGFOR 深信服科技

教育

华北电力大学
绍兴市邮电学院
西安音乐学院
陕西国际商贸学院
中国矿业大学
广州工商学院
河北环境工程学院
南京审计大学金审学院
广西医科大学
广州东华职业学院
合肥财经职业学院
嵊州教育局
越秀区教育局
……

医疗

威海市文登区人民医院
吉林市人民医院
金沙县人民医院
农四师医院
浙大医学院附属第一医院
温州医科大学附属第一医院
安徽医药大学第二附属医院
广东药科大学附属第二医院
菏泽医专附属医院
通辽市民族大学附属医院
东莞市卫生局
高州妇幼保健院
威海市中医院
历城区中医院
……

公检法司

务川县人民法院
汉中市勉县人民法院
蚌埠市中级人民法院
高邑法院
九江市法院
昭平县检察院
无锡市滨湖区检察院
福州市公安局
温州市公安局鹿城区分局
余杭区公安局
甘肃省监狱管理局
广东省番禺监狱
杭州市南郊监狱
……

政府

湖北省财政厅
珠海市财政局
怀化市鹤城区财政局
浙江省环保厅
广东省环境监测中心
昆明市环保局
石家庄社保局
佛山市社保基金管理局
江门统计局
福建省统计局
广西区水利厅
济源市审计局
东莞市卫生局
宝鸡市政府
……

部分成功案例

SANGFOR 深信服科技

传媒/水务	制造/运输/金融	其他
海南视听网络电视有限公司	驻马店卷烟厂	华润(集团)有限公司
杭州文化广播电视集团	中国医药集团总公司	广东侨鑫集团
通辽日报社	中山迪欧家具实业有限公司	重庆中冶建工集团
深圳广播电影电视集团	石家庄以岭药业股份有限公司	广州电力机车有限公司
海洋报社	广东江中高速公路有限公司	均瑶集团
人民邮电报社	烟台交运集团	中铁十七局集团
西藏日报	威海交通运输集团有限公司	科大国创软件股份有限公司
福建省日报社	广深珠高速公路有限公司	山西中科曙光云计算科技有限公司
威海市水务集团有限公司	广深珠高速公路有限公司	河南省脱颖实业有限公司
厦门水务集团	浙江股权交易中心	中金花桥数据系统有限公司
江阴市江南水务	石家庄市股权交易中心	北京此时此地信息科技有限公司
临海水务集团	英大基金	冠丰房地产开发有限公司素凯泰酒店
……	……	……

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

日志审计系统LAS（联合开发）

产品概述

深信服LAS日志审计系统基于嵌入式64位Linux系统，由日志采集模块、事件检索模块、审计报表模块、综合管理模块组成。采用B/S架构，管理员通过HTTPS方式对主机进行管理

日志采集方式：

- ✓ 标准协议：采集SYSLOG、SNMP_TRAP、OPSEC_LEA协议类日志信息；
- ✓ 网络抓包：通过旁路侦听解析数据包，形成网络访问行为日志记录；
- ✓ 日志文件：通过专用脚本上传信息系统中存在的各类日志文本；

审计对象类型：

- ✓ 操作系统：Windows、LINUX、AIX、HP-UX、SCO UNIX、SOLARIS…
- ✓ 网络设备：交换机、路由器、负载均衡、代理设备…
- ✓ 安全设备：防火墙、IDS/IPS、UTM、防病毒墙、VPN…
- ✓ 应用系统：WEB Server、FTP Server、MAIL Server、WebLogic、Tomcat…
- ✓ 数据库操作：Oracle、DB2、MSSQL、SyBase、MySQL、Informix…
- ✓ 网络访问行为：网页浏览、BBS、文件传输、邮件收发、IM聊天、BT…

产品功能

日志采集

支持所有日志类型采集，Windows、Linux、交换机、数据库及应用日志等。

实时分析

根据策略实时分析告警，实时告知用户服务器运行状态。

日志检索

通过日志中的关键字段快速检索定位

关联分析

连续多次密码错误即判断为暴力破解，通知管理员

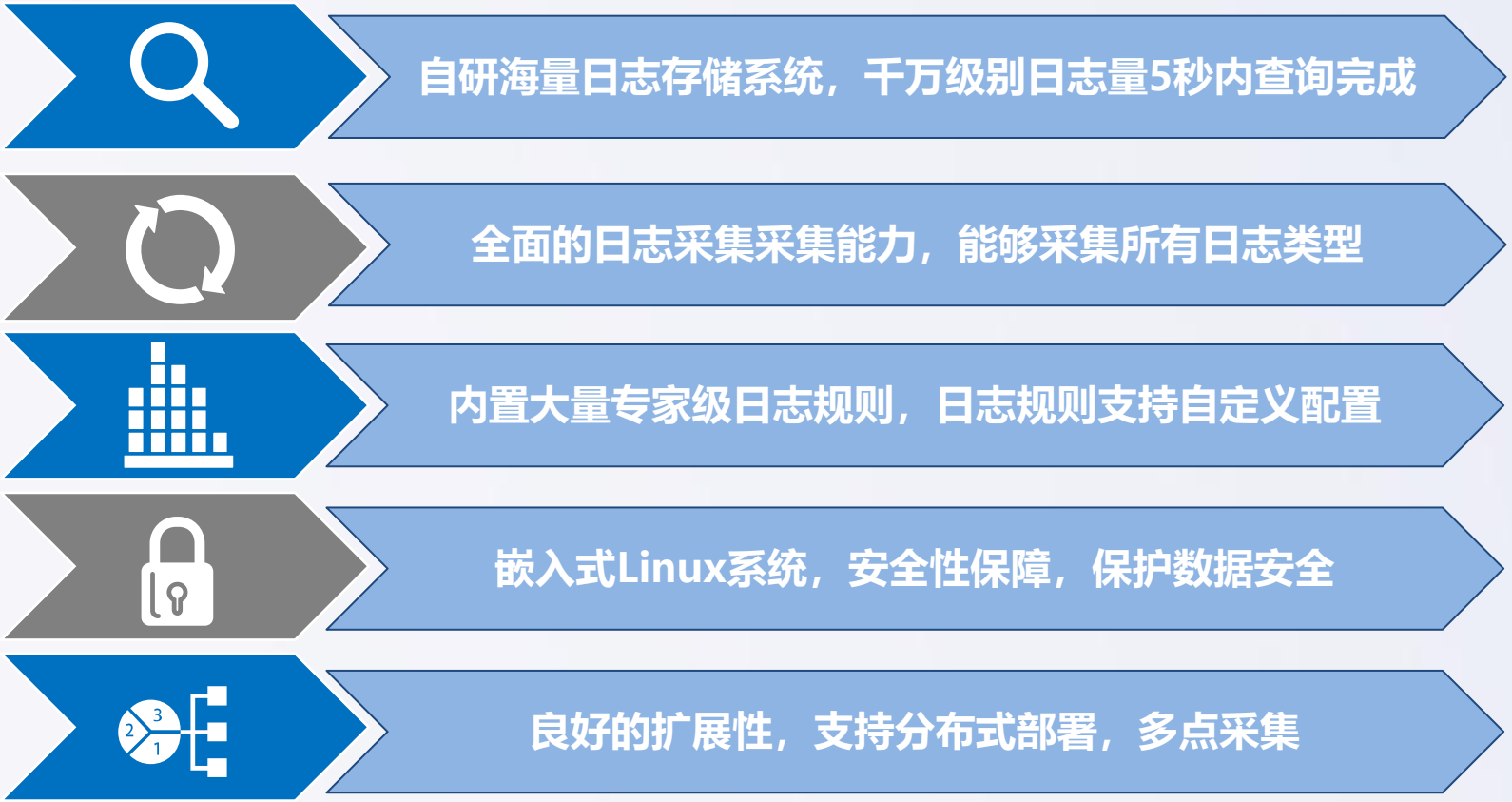
审计报表

根据用户情况周期生成报表，分析运行状态及安全事件

安全存储

日志统一集中安全存储， 防止日志被删与丢失

技术优势


自研海量日志存储系统，千万级别日志量5秒内查询完成
全面的日志采集采集能力，能够采集所有日志类型
内置大量专家级日志规则，日志规则支持自定义配置
嵌入式Linux系统，安全性保障，保护数据安全
良好的扩展性，支持分布式部署，多点采集

客户价值

集中统一管理

无需登录每个系统
即可统一查询管理所有日志

实时动态分析

根据日志等级与信息内容自定义规则
实时告警通知管理员，及时发现问题与故障

安全合规

满足二级等保与行业合规需求

日志留痕防篡改

保障日志数据安全
防篡改防删除设计

快速检索定位

根据日志关键字段快速检索定位
还原问题与故障缘由

综合报表分析报告

自定义报表，统计分析日志信息
了解运维安全势态，发现安全隐患

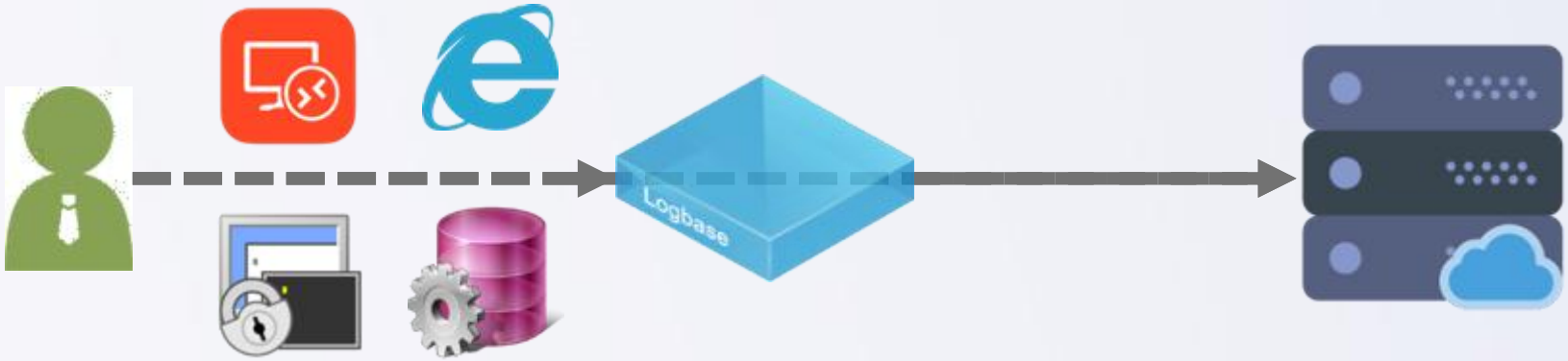
SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

堡垒机（联合开发）

产品概述

简单来说—深信服堡垒机是一套多维度的运维操作管控与审计的安全设备，使得管理人员可以全面对各种资源(如网络设备、服务器、安全设备和数据库等) 进行集中账号管理、细粒度的权限管理和访问审计、全程的运维操作审计



统一运维访问通道

运维用户不再直接访问服务器，先访问堡垒机再进行跳转。

统一人员身份认证

为用户创建独立的运维账号，人员账号一一对应，有效辨别人员身份。

统一资产管理

将网络中所有服务器资源账号信息统一安全管理，无需再对用户提供账号信息。

统一访问授权

用户只能访问他有权访问管理的服务器与资源。

产品功能

身份认证

对用户登陆运维进行身份认证，鉴别人员身份，实现责任定人。

账号管理

实现对服务器、网络设备、数据库及其帐号的统一集中安全管理。

访问控制

基于最小权限划分原则，实现集中访问控制和细粒度命令级控制。

单点登录

实现密码自动代填，运维用户无需知晓服务器账号密码，登录一次即可访问所有授权服务器。

审计记录

审计实名制，对用户从登录到退出的全程操作行为的监控和事后审计。

SANGFOR
深信服科技

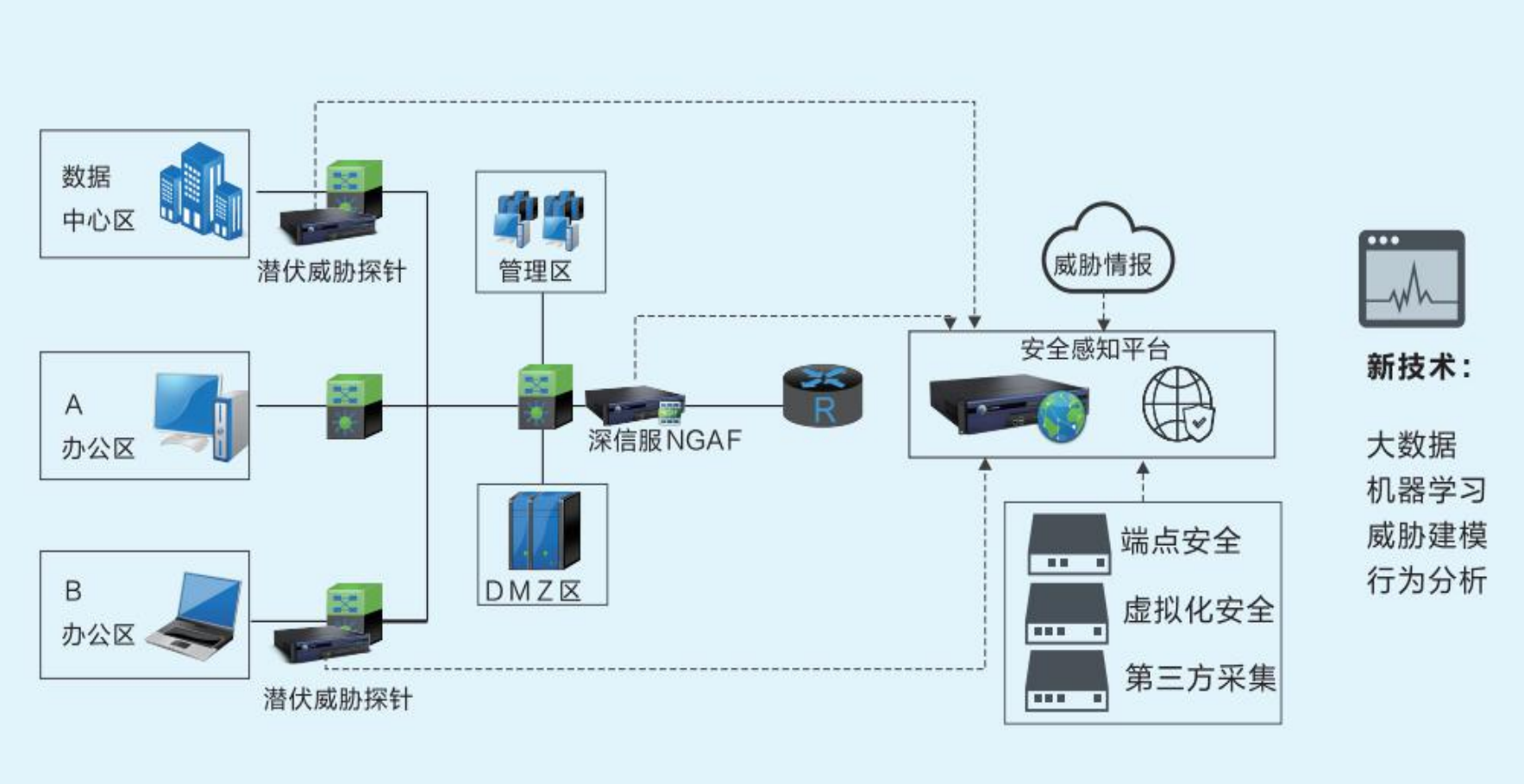
SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

深信服安全感知平台SIP

安全感知平台定位

深信服安全感知平台是以全流量分析为基础，结合威胁情报、行为分析、UEBA、机器学习、大数据关联分析、可视化等技术对全网流量实现全网业务可视化、威胁可视化、攻击与异常流量可视化，从而实现全面发现各种安全威胁



安全感知平台架构


呈现及可视化
综合安全预警
安全监控中心
大屏可视化
安全态势预警
资产中心
报表 / 报告
安全分析
MapReduce并行处理框架
关联分析
U E B A
访问关系分析
行为分析
特征匹配
违规访问
机器学习
协议分析
资产识别
人工大数据安全分析服务
安全态势
溯源分析
潜伏威胁
攻击态势
脆弱性分析
威胁预警
对外接口
第三方系统及平台
数据存储
Elastic Search存储
MongoDB存储
数据预处理
数据清洗
数据过滤
标准化
关联补齐
数据标签
采集对象
终端数据
流量数据
威胁情报
安全设备
服务器

产品功能

SANGFOR 深信服科技

数据采集

- 全流量采集
- 威胁情报
- 终端安全日志采集
- 操作系统日志采集
- 文件还原
- 云端沙箱

持续检测

- 漏洞攻击检测
- 文件威胁分析
- WEB攻击检测
- 异常行为分析
- 失陷主机检测
- UEBA基线学习
- 业务脆弱性分析
- 全攻击链关联

运维处置

- 事件响应处置
- 安全知识库
- 事件详细举证
- 联动响应
- 安全专家

溯源取证

- ES快速搜索
- 大容量存储空间
- 流量元数据存储
- 攻击入口点溯源
- 影响面分析
- 终端日志
- 操作系统日志

传统安全防护体系的三个弊端

01 安不安全不知道

- 安全设备没有告警，就没有问题了？
- “敌暗我明”，不是看不到问题就没有问题！

02 哪里不安全不知道

- 黑客到底是怎么黑进来的？
- “盲人摸象”，缺乏有效的手段检测多变的攻

03 造成了什么危害不知道

- 办公服务器被黑了，修复好它之后，问题就解决了吗？
- “防不胜防”，跳板攻击控制核心业务，信息泄露而不自知！

我们寄希望于

检测率高

不仅能够识别已知威胁还能识别0day 、APT、未知恶意威胁

实用性强

1）能够通过大数据分析系统识别攻击是否真实发生、攻击是否成功、证据充分，能够提供详细的佐证材料
2）查询速度快不卡顿
3）可用性强，不宕机
4）对确认的安全风险，可自动闭环处理

美观溢价

1）可视化界面美观
2）无需定制，和业务需要匹配度高
3）重点突出，呈现效果好

优势点①：纵深检测模式，检测率高

公司战略投入大量安全研究人员持续不断的研究最新的安全威胁，提升态势感知系统的检测能力。对于可疑数据包，我们采用四层纵深检测模式，分别进行特征匹配、威胁情报关联、病毒引擎鉴定，对于仍未能识别的可疑数据包我们采用SAVE引擎智能识别技术

特征库

- 9500+漏洞利用攻击特征
- 3000+WEB应用攻击特征
- 35W+僵尸网络特征
- 百万恶意URL地址库

威胁情报

- 深信服云脑平台
- Google Virustotal
- CNCERT、CNVD
- Malwaredb等开源情报

文件鉴定

- 国内病毒引擎（EDR-火绒）
- 国外引擎检测（EDR-小红伞）
- 开源引擎检测（ClamAV）
- 云端文件信誉匹配

采用SAVE检测引擎，智能识别高危未知威胁

SANGFOR 深信服科技

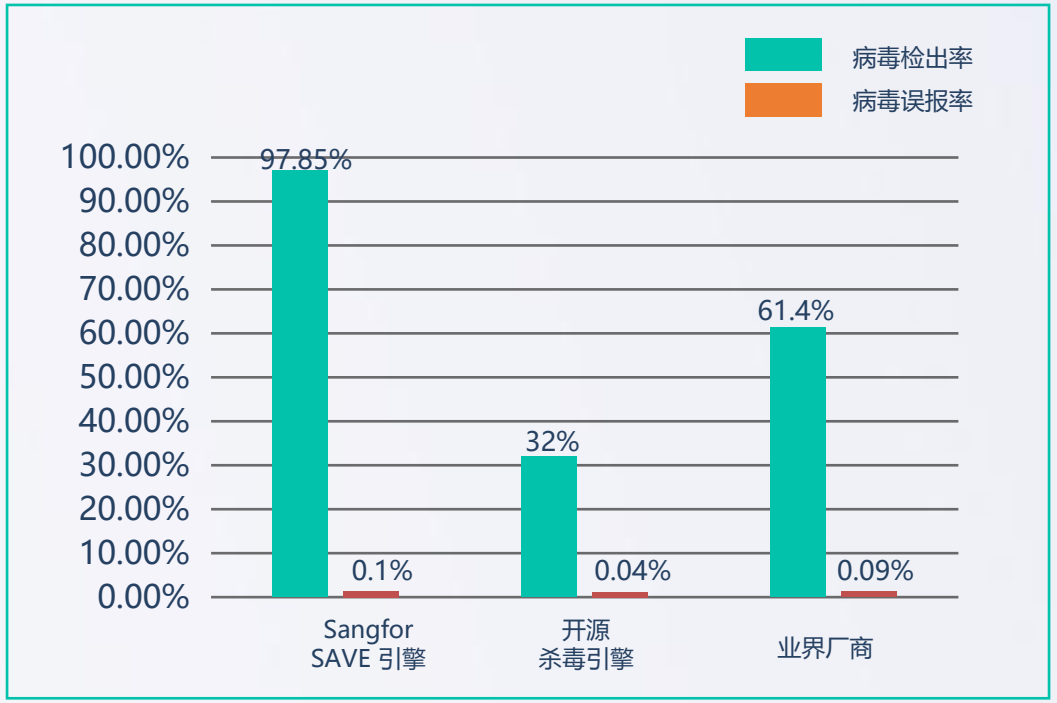
深信服人工智能检测引擎SAVE

SANGFOR AI-based Vanguard Engine

创新人工智能无特征技术
准确检测未知病毒

Wannacry、Badrabit 、
GlobeImposter及其变种
100%查杀

泛化能力强



低误报、高检出

权威机构认可

采用SAVE检测引擎，智能识别高危未知威胁

SANGFOR 深信服科技

文件头

dll函数名 | dll文件名

信息熵 | 小波变换

..... | .....

文件节

数据特征 | API调用

IO访问 | 函数关联

..... | .....

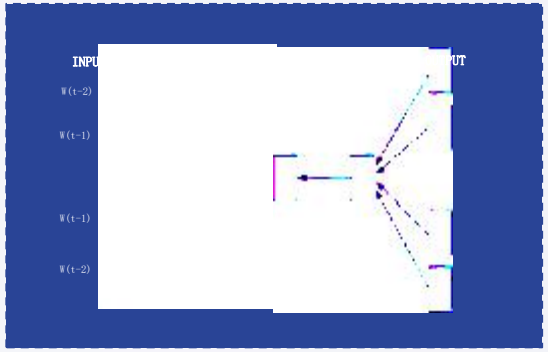
文件证书与资源

数字签名XXX

Version XXX

Company XXX

特征向量编码



特征工程

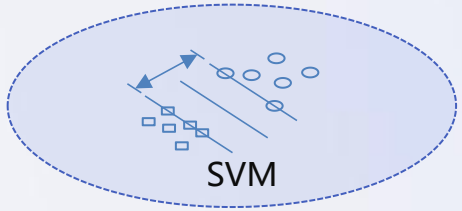
特征池

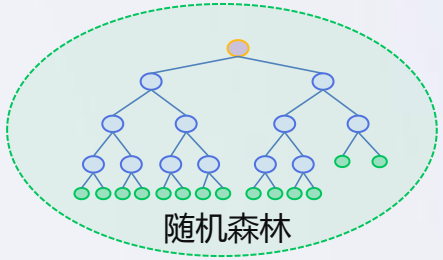
信息增益 | Fisher Score

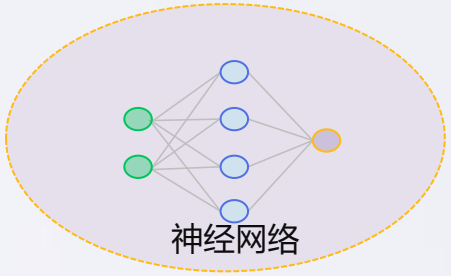
mutual info | Wrapper

W(t-1)

综合多种分类算法+集成学习





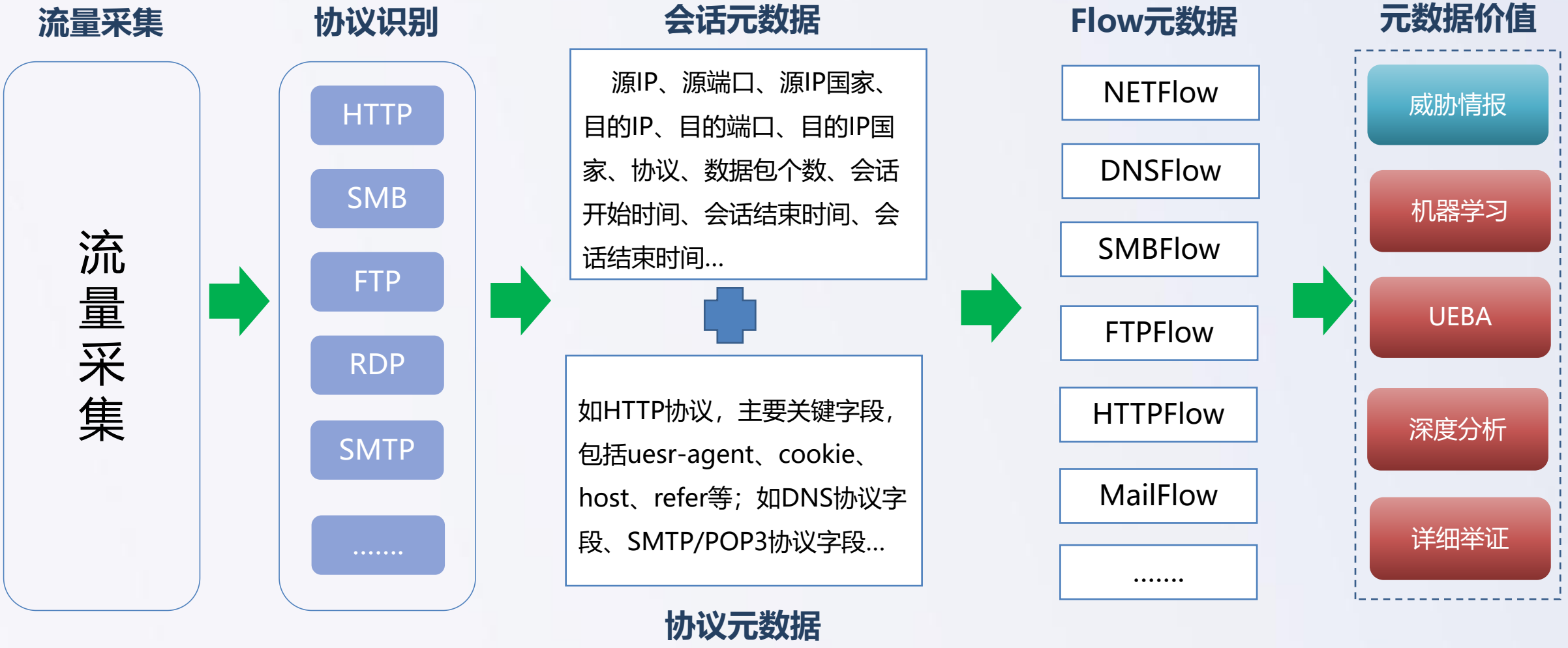


恶意文件

正常文件

优势点②：采用全流量技术 详细举证 实用性强

SANGFOR 深信服科技

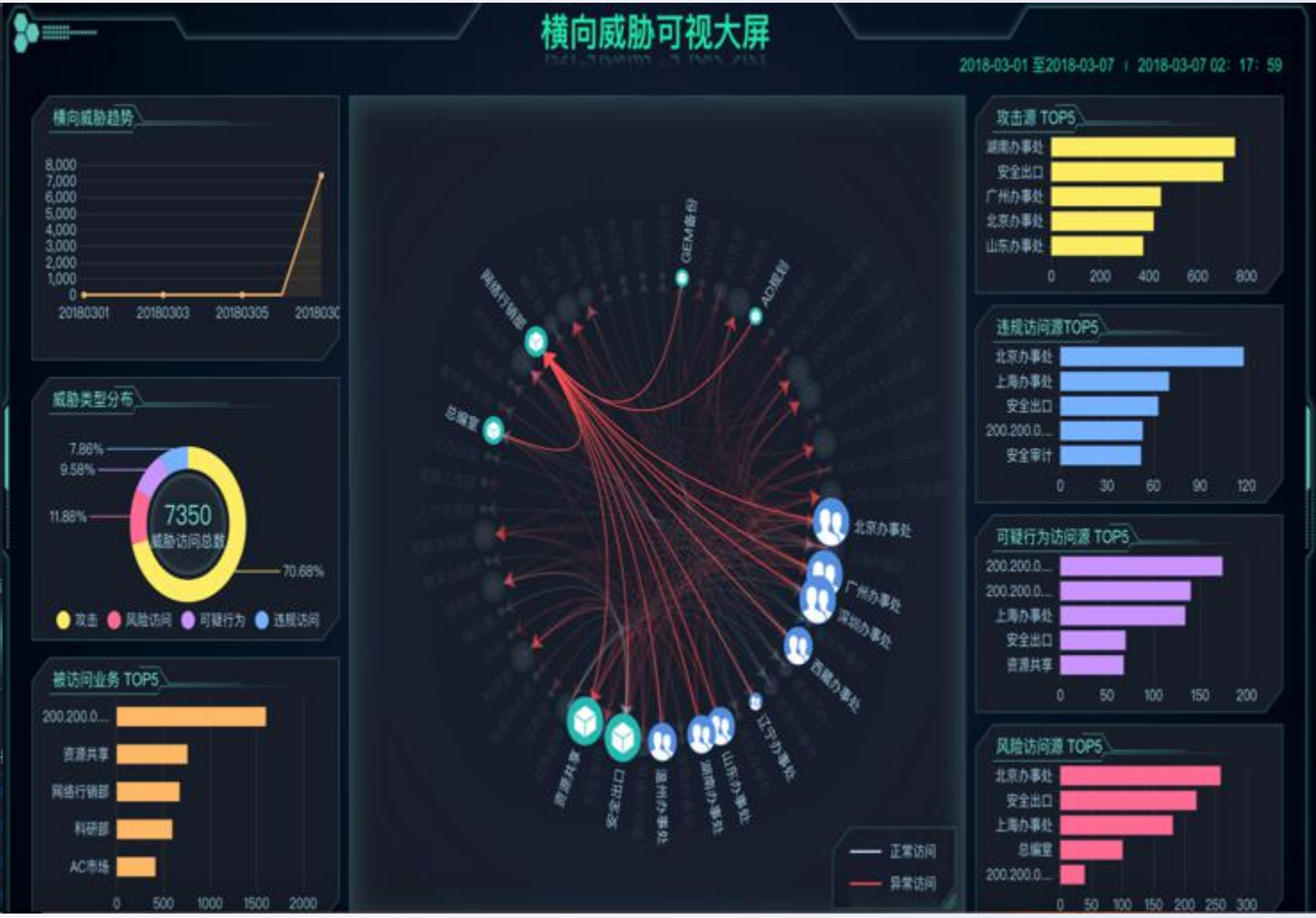


详细举证案例


刷新
刷新
概况
服务器IP： 200.200.88.88
所属业务： -
所属分支： -
攻击阶段分布：
5
遭受入侵
15
C&C
内网
该服务器疑似被黑客控制，对互
法规、被网安等监管单位通报，
举证
开放端口
全部阶段
全部失陷等
7 主机多次访问由DGA生成的恶意软件C... 随机域名行为分... C&C通信 已失陷 中威胁 2017-08-10 02:17:15
详细信息 风险危害 处理建议
访问趋势（次）
10
5
0
07-12 07-14 07-16 07-18 07-20 07-22 07-24 07-26 07-28 07-30 08-01 08-03 08-05
1、主机访问由DGA生成的恶意软件C&C域名，共访问5次，域名包括：aus23z4df232.net等，控制者IP（TOP3）：2.16.168.120（俄罗斯，5次）；
07-12 07-17 07-22 07-27 08-01 08-06
7 主机多次访问由DGA生成的恶意软件C... 随机域名行为分... C&C通信 已失陷 中威胁 2017-08-10 02:17:1
详细信息 风险危害 处理建议
1、如果主机是服务器，确认是否有DNS服务、邮件服务或者其它代理服务，如有则进一步确认所访问的恶意域名是否由代理服务发出来的；
2、如果流量是由代理服务发出来的，则通过抓包确认内网真实中毒主机即可，并优先使用飞客蠕虫专杀工具进行清理；
3、如果主机是普通PC，或服务器无相关代理服务，则建议优先使用飞客蠕虫专杀工具进行查杀；
4、如果飞客蠕虫专杀工具查杀不出来，建议再使用杀毒工具进行查杀；
5、建议打上MS08-067漏洞补丁包，并且更新所有的安全补丁包，保持及时更新；
6、关闭不必要的服务或端口，开启本地防火墙功能，避免再次感染。

优势点③：美观溢价


外连风险监控
国际
国内
外连国家TOP5
美国 4775
荷兰 1389
哥伦比亚 1098
日本 848
英国 764
总部
风险外连
0-499
500-999
1000-1499
1500-1999
≥2000
攻击 违规访问 APT C&C通信 可疑行为 服务器风险访问 隐蔽通信
外部IP（个） 78 10 42 7 16 16
访问次数 7375 1348 2761 920 906 596
俄罗斯
日本
哥伦比亚
马来西亚
最新事件
发生时间 源 目的 风险类型 等级 描述 状态
2018-03-07 01:07:05 200.200.0.9(腾讯通) 161.132.0.1(秘鲁) 违规访问 低危 违反白名单策略: test1 已拦截
2018-03-07 17:04:20 200.200.0.6(信息... 60.62.62.62(日本) 服务器风... 低危 使用远程桌面应用进行远程... 已拦截
2018-03-07 07:53:14 200.200.0.7(科研部) 200.10.100.1(阿... 服务器风... 低危 直接访问后台Oracle数据库... 已拦截
2018-03-07 22:39:22 200.200.0.10(版... 24.232.0.1(阿根廷) 违规访问 低危 违反白名单策略: test1 已拦截


横向威胁可视大屏
2018-03-01 至2018-03-07 | 2018-03-07 02: 17: 59
横向威胁趋势
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
20180301
20180303
20180305
威胁类型分布
7.86%
9.58%
11.88%
70.68%
7350
威胁访问总数
攻击 风险访问 可疑行为 违规访问
被访问业务 TOP5
200.200.0...
资源共享
网络行销部
科研部
AC市场
0 500 1000 1500 2000
攻击源 TOP5
湖南办事处
安全出口
广州办事处
北京办事处
山东办事处
0 200 400 600 800
违规访问源TOP5
北京办事处
上海办事处
安全出口
200.200.0...
安全审计
0 30 60 90 120
可疑行为访问源 TOP5
200.200.0...
200.200.0...
上海办事处
安全出口
资源共享
0 50 100 150 200
风险访问源 TOP5
北京办事处
安全出口
上海办事处
总编室
200.200.0...
0 50 100 150 200 250 300
正常访问
异常访问

宏观可视辅助决策

资产脆弱性态势

网络攻击态势

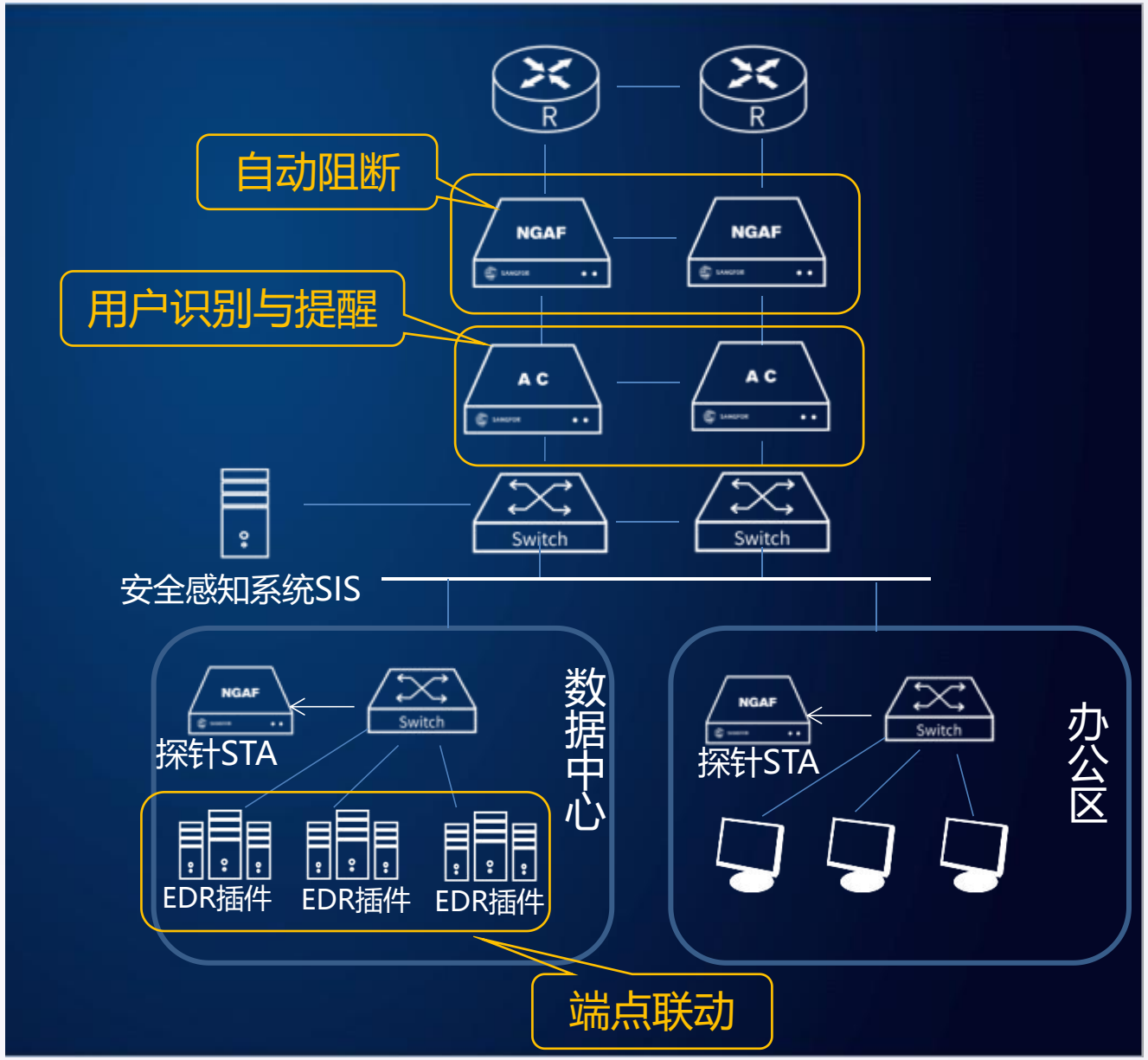
横向威胁态势

综合安全态势

外连风险态势

安全事件态势

优势点④：云网端联动-快速响应 积极防御



- **自动阻断**：自动阻断木马与黑客通信
- **端点联动**：端点执行扫描、查杀等动作
- **用户识别与提醒**：识别用户身份，封堵后页面提醒
- **高级人工服务**：**安全**应急响应，解析网络威胁，并给出安全建设建议

客户价值

看清业务

看清IT资产

业务逻辑可视

看到威胁

威胁情报关联

未知攻击检测

看懂风险

安全运维可视

有效攻击分析

辅助决策

攻击行为展示

安全态势可视

客户案例

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

金融行业	中国银联 China UnionPay；中信银行 CHINA CITIC BANK；新网银行；东北证券
国家部委	中华人民共和国国务院新闻办公室 The State Council Information Office of the People's Republic of China；中华人民共和国自然资源部 Ministry of Natural Resources of the People's Republic of China；中华人民共和国审计署 National Audit Office of the People's Republic of China；中华人民共和国国家新闻出版广电总局
政府行业	广东省人民政府 People's Government of Guangdong Province；河北省人民政府 THE PEOPLE'S GOVERNMENT OF HEBEI PROVINCE；北京市公安局 对党忠诚 服务人民 执法公正；重庆市气象局 Chongqing Meteorological Bureau
教育行业	復旦大學 Fudan University；浙江大學 ZHEJIANG UNIVERSITY；静安教育信息网 Jingan Education Information Network；南山区教育局
医疗行业	上海市卫生和计划生育委员会 Shanghai Municipal Commission of Health and Family Planning；浙江省卫生健康委员会 HEALTH COMMISSION OF ZHEJIANG PROVINCE；复旦大学附属肿瘤医院 Fudan University Shanghai Cancer Center；山东大学齐鲁医院 QILU HOSPITAL OF SHANDONG UNIVERSITY
企业	中国中车 CRRC；华润；中国葛洲坝集团有限公司 CHINA GEZHOUBA GROUP COMPANY LTD.；众泰汽车 ZOTYE AUTO

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

行为感知平台BA

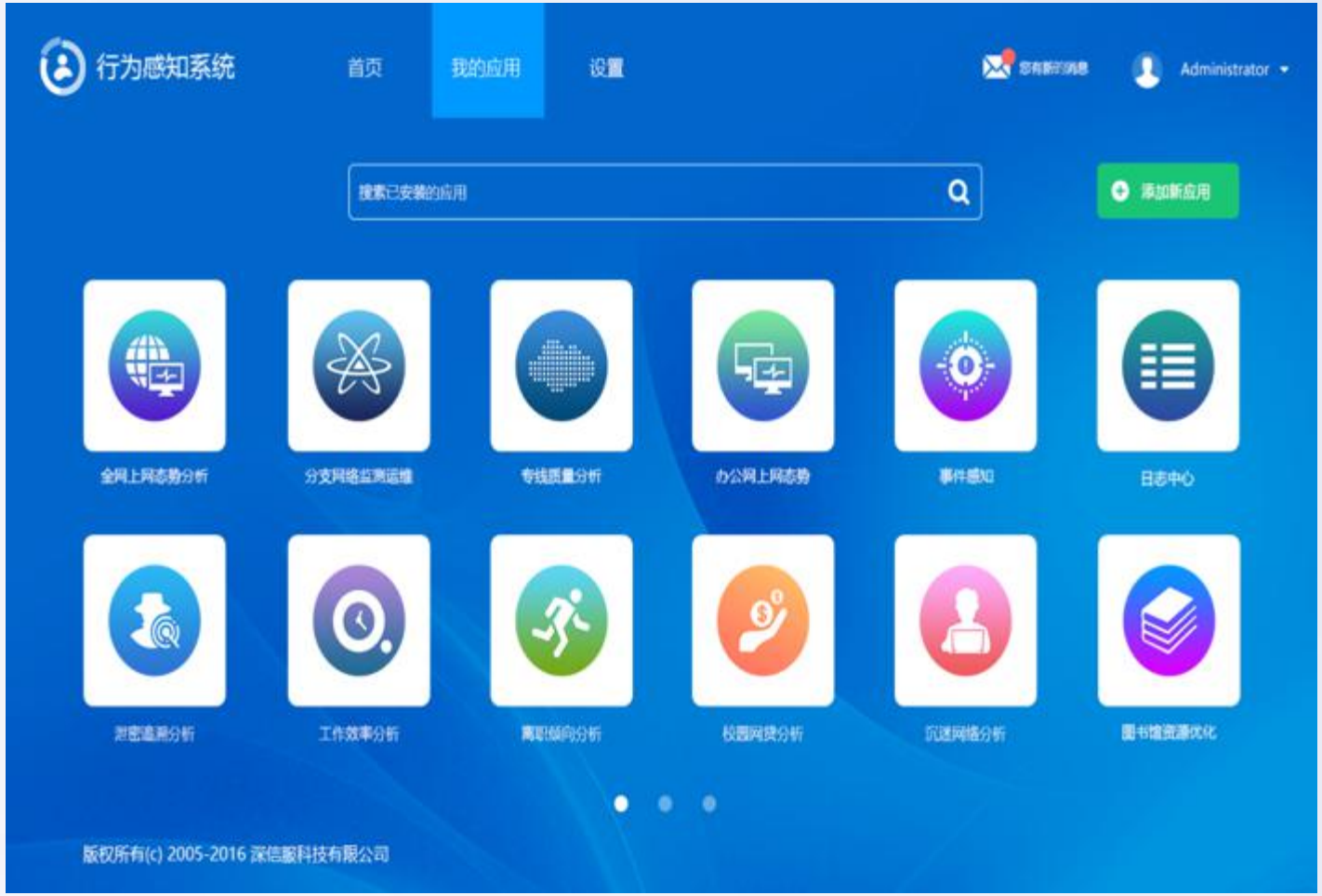
产品概述

深信服行为感知系统

是一款同深信服上网行为管理高度耦合的大数据分析系统，是一款自主研发、高性能、高可用和高扩展性的的数据计算与服务的平台

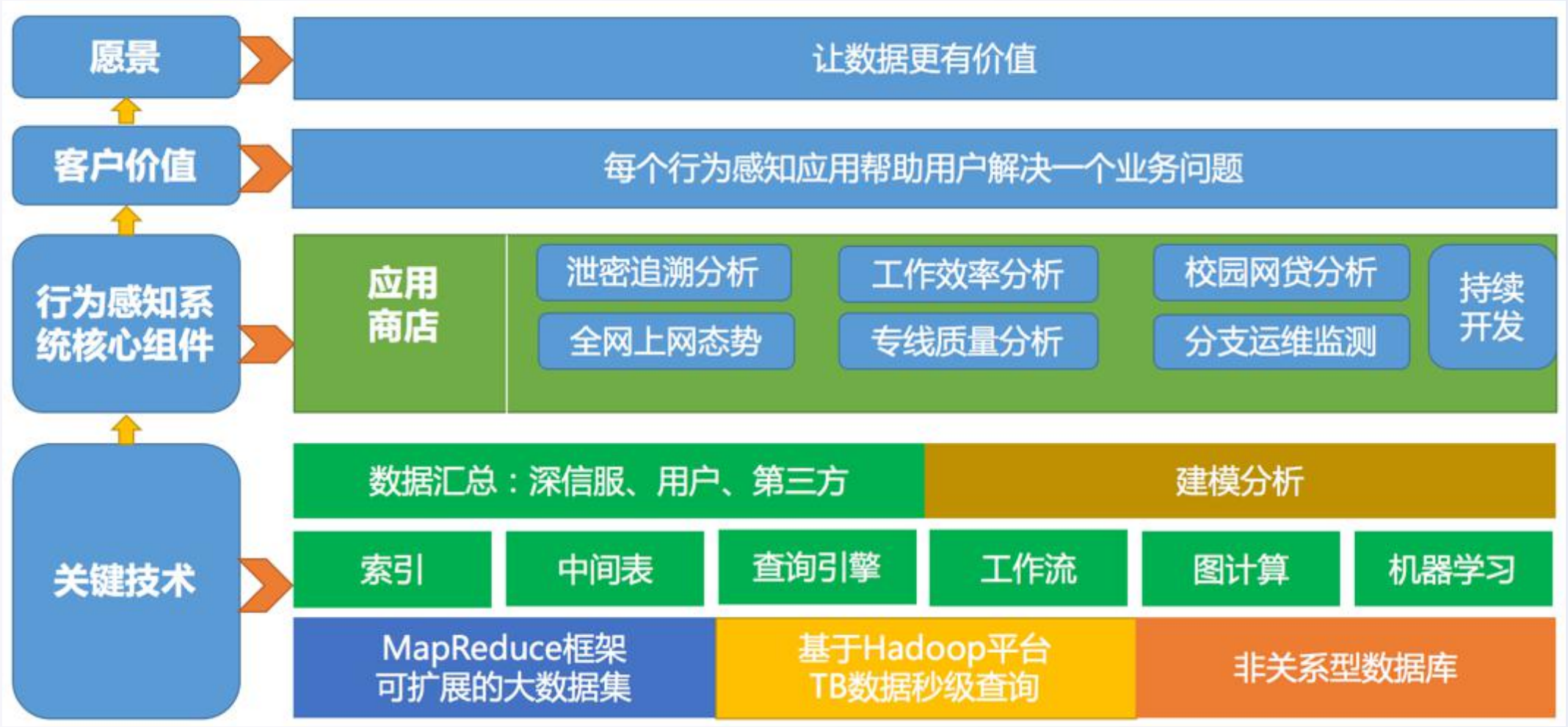
- ✓ 全新技术架构
- ✓ 基于不同场景的数据分析应用
- ✓ 面向户行为特征进行深度建模分析

价值理念：让数据更有价值，简化网络运维管理，发现组织行为风险，辅助决策/优化服务质量、提升组织效率



深信服行为感知系统3.0面向总部-多分支场景/组织行为风险分析两大场景，先后已经发布了13款行为感知应用

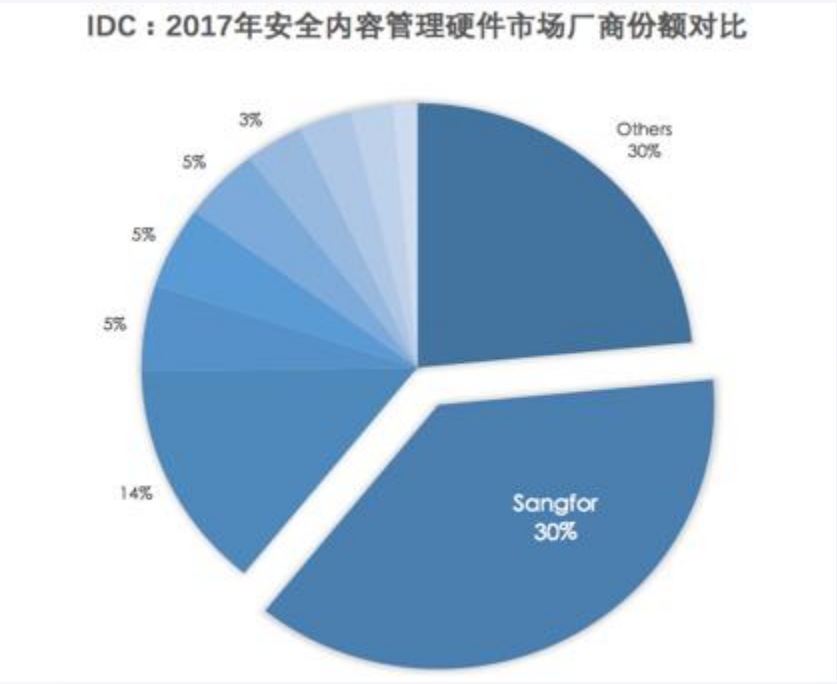
产品架构



采用分部署大数据架构设计，秒极查询；在部署上，上网行为管理负责收集数据
行为感知系统负责汇总和分析数据

技术优势

因为专注 所以专业



创新推出上网行为感知系统

先后发布了13款行为感知应用，不断探索新场景的应用，持续挖掘数据价值。

内容安全市场占有率第一

2017年市场占有率30%，超第2和第3名的总和 ;拥有全国最完善的应用识别特征库和URL库

提供多选择

会识别很多外发的危险特征，提供丰富的选择给用户，比如用户外发了加密文件，把重要资料发给竞争对手或跨越国境。

支持应用商店快速选购部署

基于BA的APP应用可直接在应用商店选择部署，并支持自动升级已安装的应用。

应用价值

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

数据泄密分析

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

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

全网上网态势分析

应用背景

- 多分支网络庞大，运维管理复杂
- 整体网络状况不可视

应用介绍

- 汇总实时数据，在总部统一呈现上网现状及安全现状
- 用户全局掌控全网态势以及各个分支状况

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

集中管理平台BBC

集中管理平台BBC产品概述

BBC是面向集团分支机构的运维管理的解决方案，BBC集中管理平台可以软件交付灵活部署云端或企业私有云，也可以通过一体机的方式进行交付。通过总部部署BBC集中管理平台，智能完成分支深信服全产品线设备的集中管理，实现分支零IT，运维全集中。

首页地图

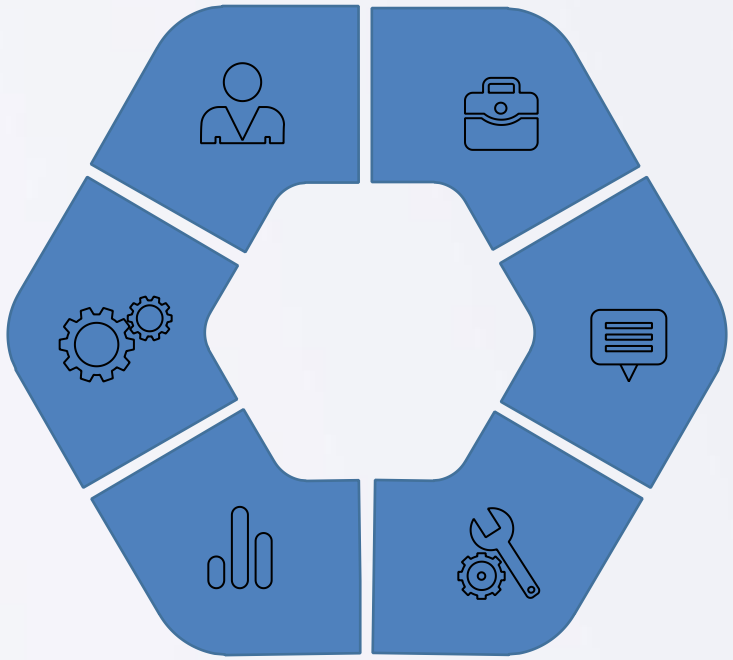
地图方式展示分支分布概况
大屏实时展示关键网络状况

智能监控

监控分支设备包括上下行流量，带宽利用率等关键参数

智能告警

分支网络告警、分支离线、授权告警、资源告警、安全告警五维度告警



报表分析

根据预设周期进行月、周、日网络情况纵览，以可视化报表等方式回溯网络情况

分支设备管理

网络设备配置统一下发
软件版本库实时更新
分支设备简易部署，快速上线

远程接入分支

总部管理人员可以远程接入分支动态调整策略
分支故障，可以快速定位故障，降低业务中断时间

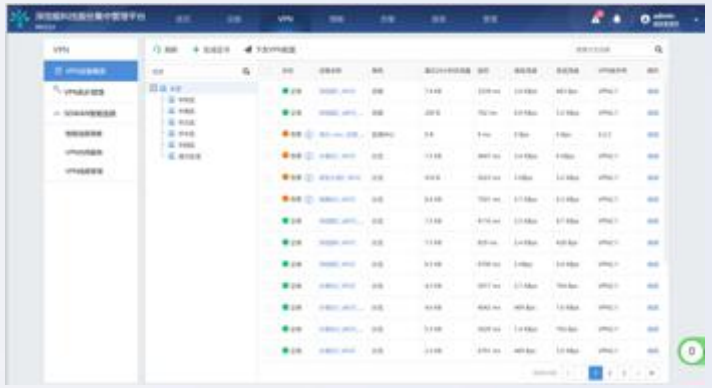
构建可视化广域网运营中心，提升运维效率

全网可视化运维

VPN可视化

4G/WIFI云易部署、邮件开局快速上线

分支CPE设备监控告警



统一配置策略下发

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

深信服威胁分析与处置服务（MDR）

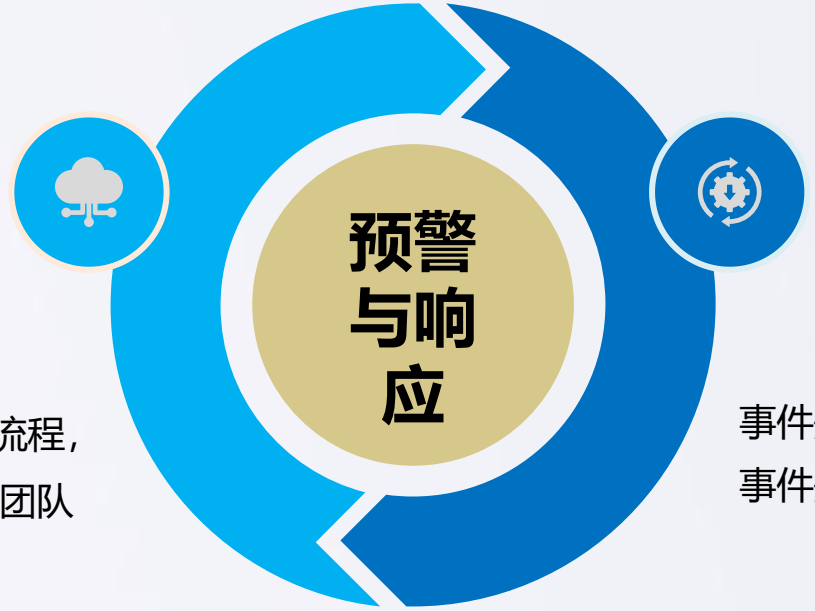
MDR服务目标

明确威胁预警与响应服务目标

对安全威胁进行有效应对，做到事前分析、预警和处置；事中标准流程应急和处置；事后溯源分析，命中目标，给出**合理性**加固建议。

MDR服务内容

通过人机共治的方式，缩短威胁响应周期，由专业的云端安全专家和应急响应专家团队为客户提供全网安全态势感知和威胁分析的检测响应闭环服务。



云上安全预警服务

持续监测与分析

云端SSP智能平台持续监测，智能分析异常流程，对风险及威胁行为生成工单，安全专家阶梯团队介入分析和验证。

威胁预警

结合“人机共智”分析结果，对已确认风险及威胁行为，通过多种机制预警用户及响应团队。

威胁告警

对于失陷主机及安全事件，通过多种机制告警用户及响应团队。

线下安全响应服务

事件处置

事件处置分为被动云端预警事件处置、威胁告警事件处置和主动定期套餐服务处置。处置方式为远程和上门两种形式。

威胁溯源

针对云端安全事件告警和主动定期套餐服务的增值服务，溯源造成事件的原因或事件源头。

安全加固建议和工作汇报

结合事件处置情况和溯源结果，给出针对该类事件处置加固建议、源头加固建议和事件产生原因加固建议。并对本次服务进行汇报

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

深信服安全运营服务（MSS）

如何构建“持续有效”的安全运营体系

SANGFOR 深信服科技

STEP 01

了解安全现状

| 安全运营现状分析|
| 安全运营成熟度评估 |

STEP 02

设计运营体系

| 安全运营框架设计 |

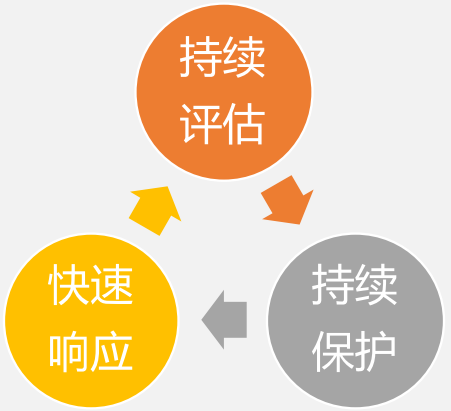
STEP 03

持续有效运营

| 资产管理，漏洞管理|
| 威胁管理，事件管理|

运营规划：采用“人机共智”的安全运营技术架构

三大运营机制



持续 闭环 主动

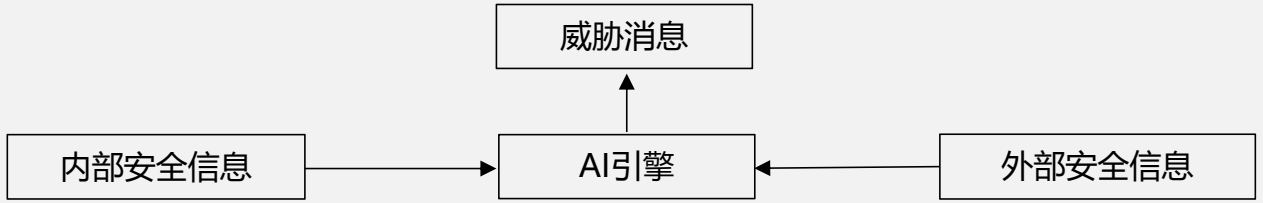
持续运营

资产管理　漏洞管理　威胁管理　事件管理

三级专家

T1工程师　T2安全运营专家　T3首席安全专家

运营中心



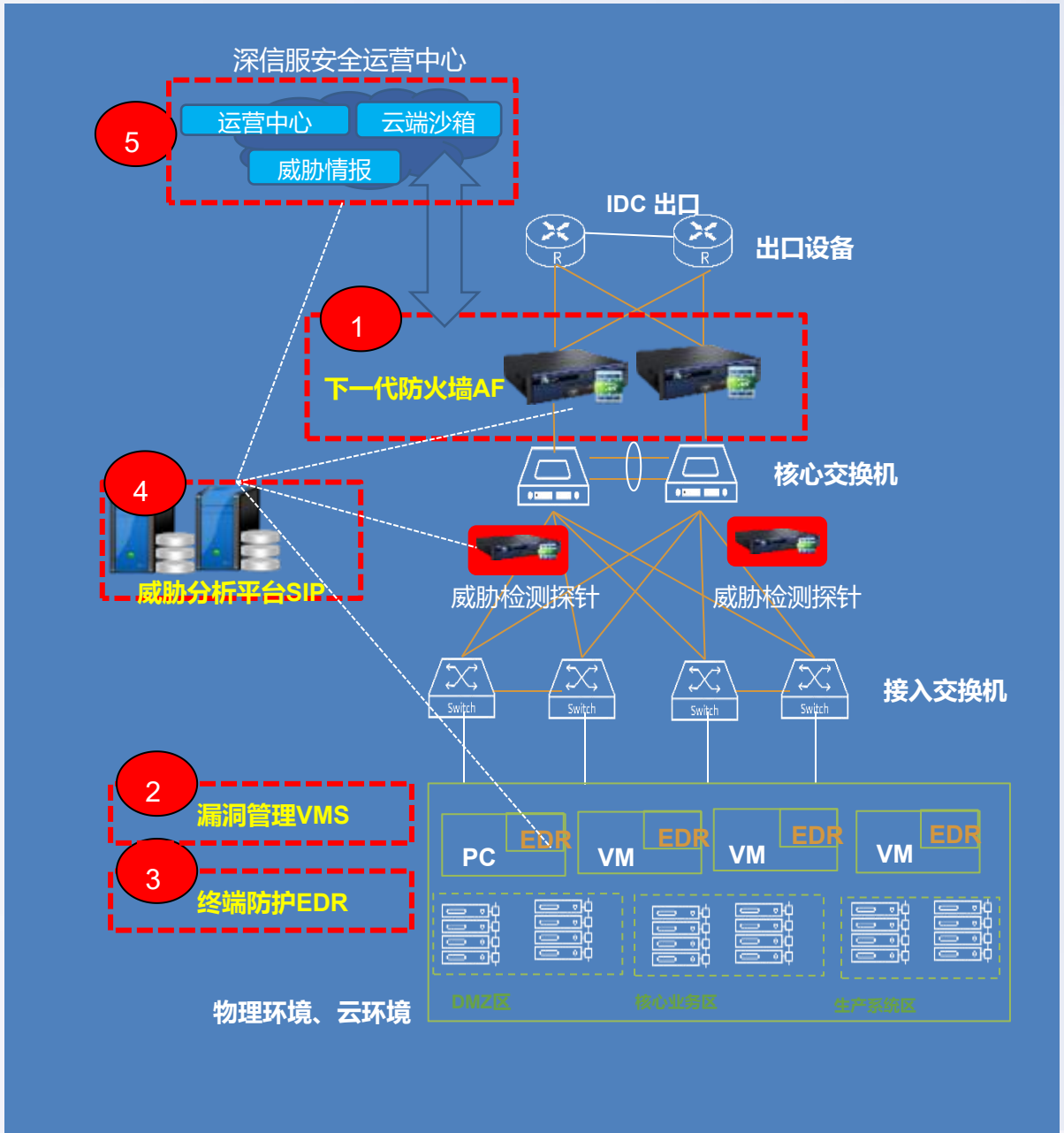
运营组件

下一代防火墙　终端检测与响应　漏洞管理平台　威胁分析平台　……

人机共智的安全运营体系，7*24小时持续为用户提供有效的安全保护

交付方式：持续运营，服务化交付

安全运营清单					
项目名称	安全运营框架		运营类型	运营方式	频率
安全运营	了解安全现状阶段		资产梳理	安全专家	按次
			暴露面监测	安全运营组件	实时
			漏洞扫描	安全运营组件	按需
			漏洞验证	安全专家	按需
			外部威胁评估	安全专家	按需
			精准入侵检查	安全专家+安全运营组件	按需
			基线检查	安全专家+安全运营组件	按次
			渗透测试（可选）	安全专家	按次
			安全现状评估报告解读	安全专家	按次
	运营体系设计阶段		安全访谈	安全专家	按次
			安全能力成熟度评估	安全专家	按次
			安全能力成熟度解读	安全专家	按次
			安全运营机制设计	安全专家	按次
			安全运营方案汇报	安全专家	按次
			安全运营方案实施	安全专家	按次
	持续有效运营阶段	漏洞管理	资产脆弱性管理	安全专家+安全运营组件	持续
			0day漏洞通告及排查	安全专家+安全运营组件	持续
		威胁管理	威胁分析与处置	安全专家+安全运营组件	持续
			策略管理	安全专家+安全运营组件	持续
			持续攻击对抗	安全专家+安全运营组件	持续
		事件管理	事件分析与处置	安全专家+安全运营组件	持续
			应急响应	安全专家+安全运营组件	持续
		运营可视	安全运营可视化	安全专家+安全运营组件	持续
			定期安全运营汇报	安全专家	按需
	其他安全服务		应急响应服务	安全专家	按次
			安全培训	安全专家	按次
			新上线业务安全评估服务	安全专家	按需
			信息安全保障设计规划咨询服务	安全专家	按次
			渗透测试服务	安全专家	按次



交付方式1-MSS+轻资产

MSS服务：

- 漏洞管理服务
- 威胁监测与主动响应服务
- 安全事件响应服务

运营组件：

① 安全运营中心VIP专属账号一套

② 安全专家7*24H微信服务群一套(T1/T2/T3)

③ 漏洞管理系统一套

④ L2-L7安全防护组件一套

⑤ 安服SIP-1000-B400一套

⑥ 安服STA-100-B420一套

⑦ 应急处置系统一套(默认含EDR授权10个)

服务期内免费使用，资产归属服务商

交付方式2-MSS+重资产

MSS服务：

- 漏洞管理服务
- 威胁监测与主动响应服务
- 安全事件响应服务

运营组件：

① 安全运营中心VIP专属账号一套

② 安全专家7*24H微信服务群一套(T1/T2/T3)

③ 漏洞管理系统一套

④ L2-L7安全防护组件一套

⑤ SIP-1000-B400一套

⑥ STA-100-B420一套

⑦ 应急处置系统一套(默认含EDR授权10个)

标红部分由客户买断

安全运营服务清单

安全运营服务清单							
项目名称	安全运营服务框架		服务类型	服务方式	服务频率	时间期限	备注
安全运营服务	了解安全现状阶段		资产梳理	安全专家	按次	1次*1年	100个资产
			暴露面监测	安全运营组件	实时		
			漏洞扫描	安全运营组件	按需		
			漏洞验证	安全专家	按需		
			外部威胁评估	安全专家	按需		
			精准入侵检查	安全专家+安全运营组件	按需		
			基线检查	安全专家+安全运营组件	按次		
			安全现状评估报告解读	安全专家	按次		
	运营体系设计阶段		安全访谈	安全专家	按次	1次*1年	100个资产
			安全能力成熟度评估	安全专家	按次		
			安全能力成熟度解读	安全专家	按次		
			安全运营机制设计	安全专家	按次		
			安全运营方案汇报	安全专家	按次		
			安全运营方案实施	安全专家	按次		
	持续有效运营阶段	漏洞管理	资产脆弱性管理	安全专家+安全运营组件	持续	7*24H*1年	100个资产 含服务组件： 1.安全运营中心账号一套 2.安全专家7*24H微信服务群一套(T1/T2/T3) 3.漏洞管理系统一套 4.L2-L7安全防护组件一套 5.安服SIP-1000-B400一套 6.安服STA-100-B420一套 7.应急处置系统一套(默认含EDR授权10个) 服务期内免费使用
			0day漏洞通告及排查	安全专家+安全运营组件	持续		
		威胁管理	威胁分析与处置	安全专家+安全运营组件	持续		
			策略管理	安全专家+安全运营组件	持续		
			持续攻击对抗	安全专家+安全运营组件	持续		
		事件管理	事件分析与处置	安全专家+安全运营组件	持续		
			应急响应	安全专家+安全运营组件	持续		
		运营可视	安全运营可视化	安全专家+安全运营组件	持续		
			定期安全运营汇报	安全专家	按需		
	其他安全服务		应急响应服务	安全专家	按次	1次*1年	按次收费
			安全培训	安全专家	按次	1次*1年	按次收费
			新上线业务安全评估服务	安全专家	按需	1次*1年	按照业务数量及次数收费；含渗透。
			信息安全保障设计规划咨询服务	安全专家	按次	1次*1年	轻量级咨询免费。重咨询按需求及规模收费
			渗透测试服务	安全专家	按次	1次*1年	按照业务数量及次数收费

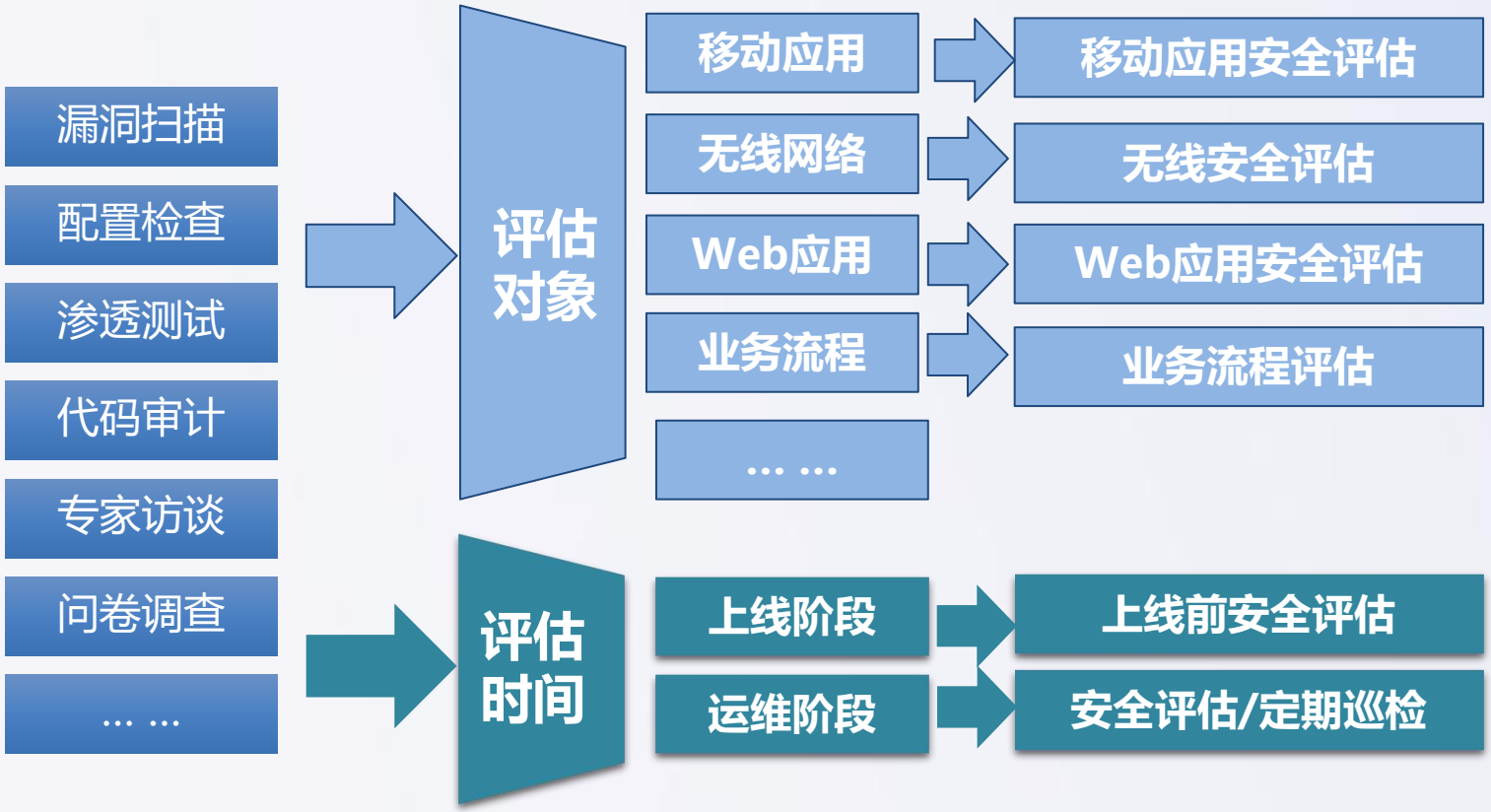
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

深信服综合人工服务（ISS）

信息系统风险评估服务

SANGFOR 深信服科技

评估方法



等保咨询服务

SANGFOR 深信服科技

定级
- 摸底调查
- 自主定级
- 新系统建设同时同步确定等级，按等级同步规划建设安全设施

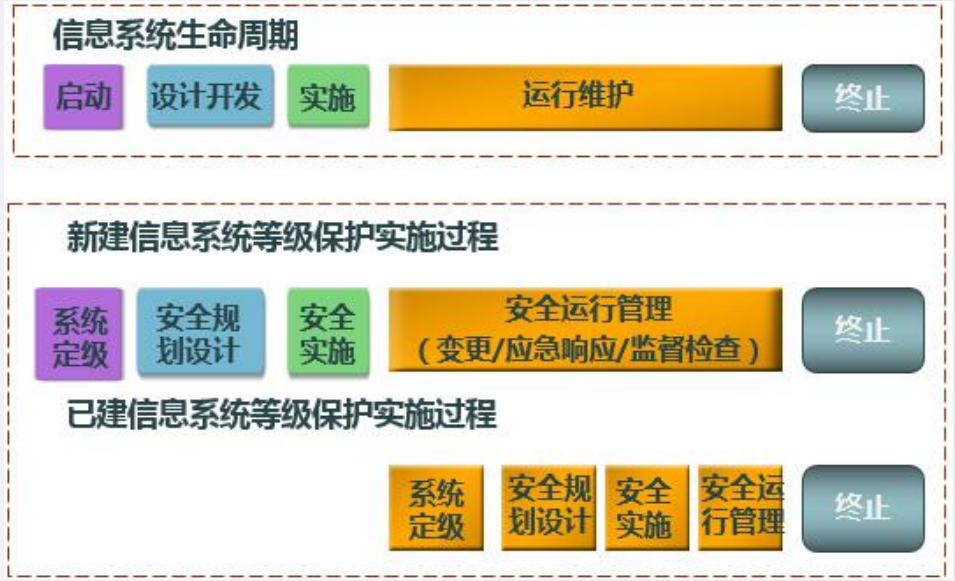
等级评审
- 专家评审
- 定级报告

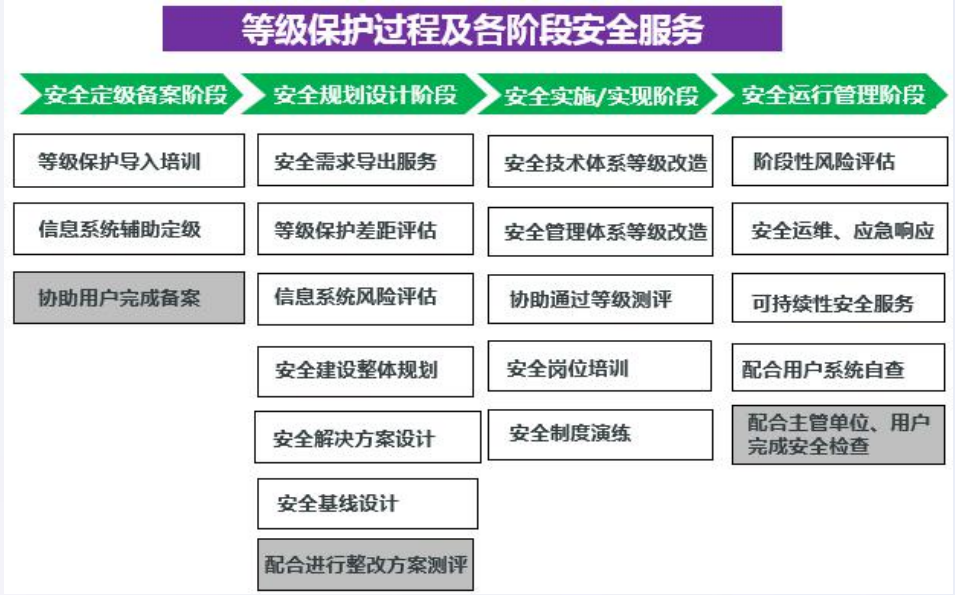
备案
- 到公安机关办理备案手续
- 涉密系统到国家保密工作部门
- 受理单位备案审核

评估和整改建设
- 评估和现状检测（可请评估或检测机构）
- 制定整改方案
- 开展安全建设或改建，建立健全信息安全等级保护管理制度

等级测评
- 开展技术测评
- 三级以上开展等级测评

监督检查
- 监督、检查、自查
- 整改
- 违法违规情况，依法处理

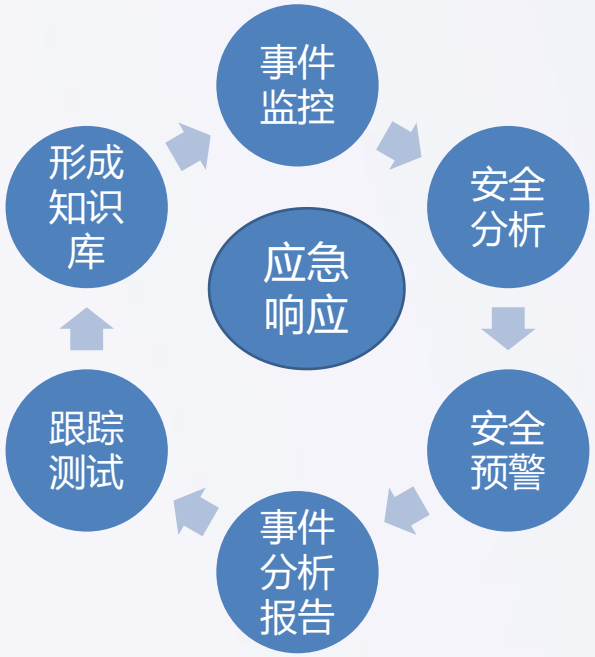




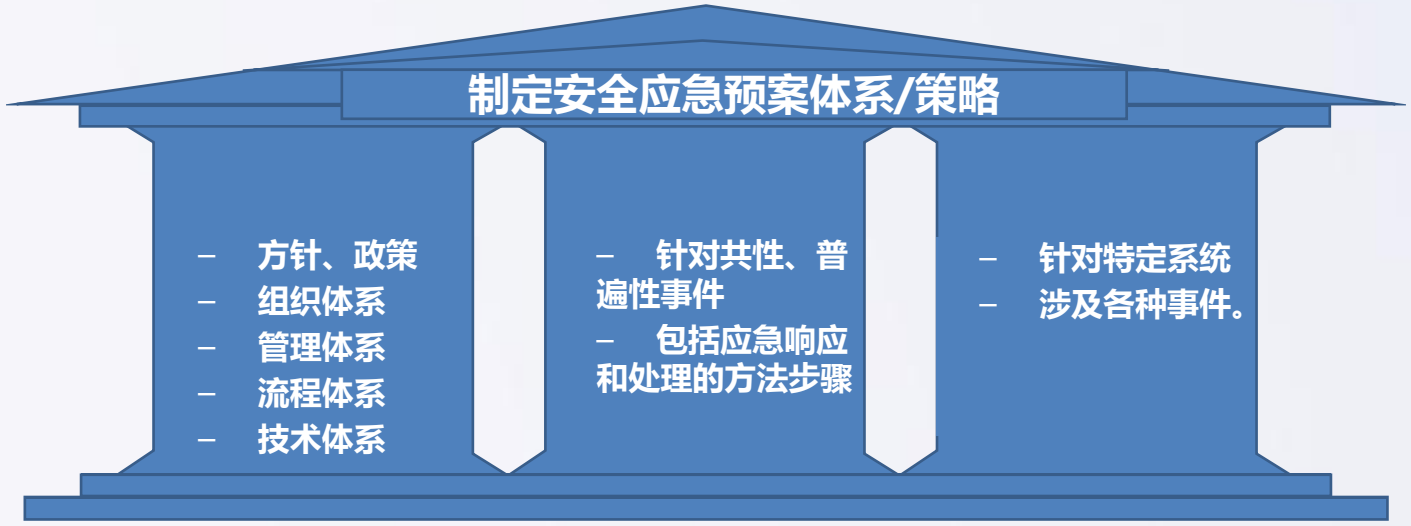
渗透测试服务


渗透测试
WEB
APP
PEN
WEB应用安全测试
Android应用安全测试
IOS应用安全测试
定向测试
✓ 网站系统安全测试
✓ 微信公众号安全测试
✓ 接口安全测试
✓ 客户端安全测试
✓ 服务端安全测试
✓ 专项安全测试（脱壳\逆向）
✓ 定点测试（传统渗透测试）
✓ 内网安全测试

应急响应&应急演练服务


事件监控
安全分析
安全预警
事件分析报告
跟踪测试
形成知识库
应急响应


应急需求确认
应急响应预案建立
应急演练
应急演练总结整改
应急演练


制定安全应急预案体系/策略
– 方针、政策
– 组织体系
– 管理体系
– 流程体系
– 技术体系
– 针对共性、普遍性事件
– 包括应急响应和处理的方法步骤
– 针对特定系统
– 涉及各种事件。

2020年深信服安全服务目录

SANGFOR 深信服科技

安全运营类服务

- 资产管理服务
- 漏洞管理服务
- 威胁监测与主动响应
- 安全事件响应
- 本地安全运营中心建设服务
- 安全通告

安全评估类服务

- 风险评估
- 渗透测试
- 漏洞扫描
- 基线核查
- 代码审计
- APP检测
- 无线安全评估

安全培训类服务

- 安全意识培训
- 安服技能培训
- CISP培训
- CISAW培训

安全规划咨询

- 安全规划咨询
- 等保咨询服务

安全运维类服务

- 应急响应
- 应急演练
- 安全加固
- 驻场运维
- 安全日志分析与响应服务

SANGFOR
深信服科技

1、产品推广工具—深信服助手

2、产品推广工具—互联网有效性评估器

两大评估场景

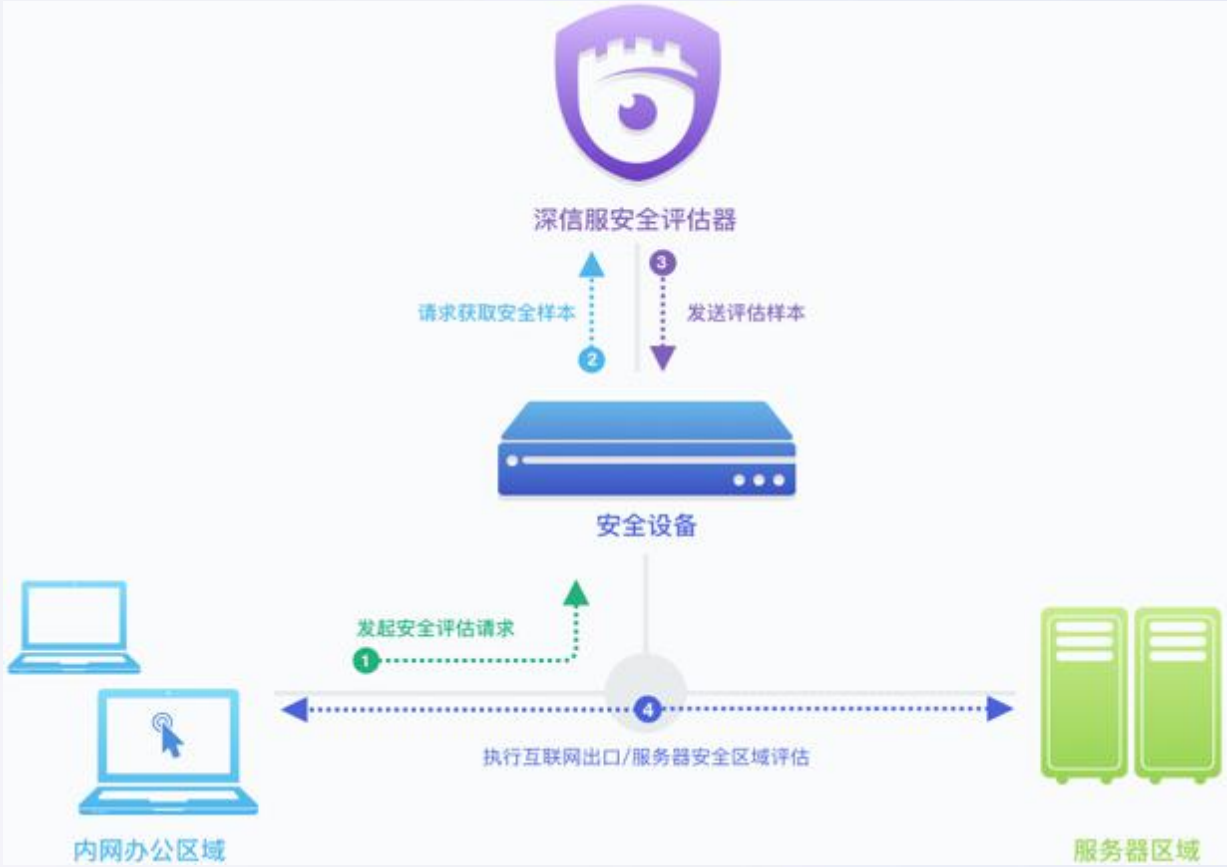
➢ 终端主机安全评估

针对员工日常工作及活动内容，评估企业在互联网出口是否有足够的安全防护能力来有效保护员工上网和日常办公的安全，避免员工遭受网络威胁的攻击，包括**防勒索病毒，防违法访问，防钓鱼攻击**等多种终端安全能力评估。

➢ 服务器出口安全评估

在服务器出口区域，针对常见外部威胁攻击进行有效评估，包括服务器**防扫描，防攻击，防控制**等多个环节，评估客户现有互联网出口安全防护体系是否能有效应对常见应用层攻击。

注：服务器安全评估功能模块目前在调整中，暂时无法提供相关安全服务



平台工作原理如上图描述，主要分为以下几个阶段：

1. 客户内部网络终端登录深信服安全评估器使用界面，发起请求评估；
2. 根据检测类型请求云端平台评估样本；
3. 云端评估平台接收请求，发送攻击特征样本到终端主机或者服务器；
4. 发送样本到终端主机会经过互联网出口边界的安全防护设备，通过此过程检测用户互联网出口是否具备相应攻击类型的防护能力；

2、产品推广工具—互联网有效性评估器

使用流程：

注册/登录账号 ⇒ 一键开始检测 ⇒ 获取检测报告 ⇒ 检测报告解读

1、登录 http://sec.sangfor.com.cn/，进入【深信服安全中心】，在界面中点击【安全有效性评估】进入评估器界面

2、产品推广工具—互联网有效性评估器

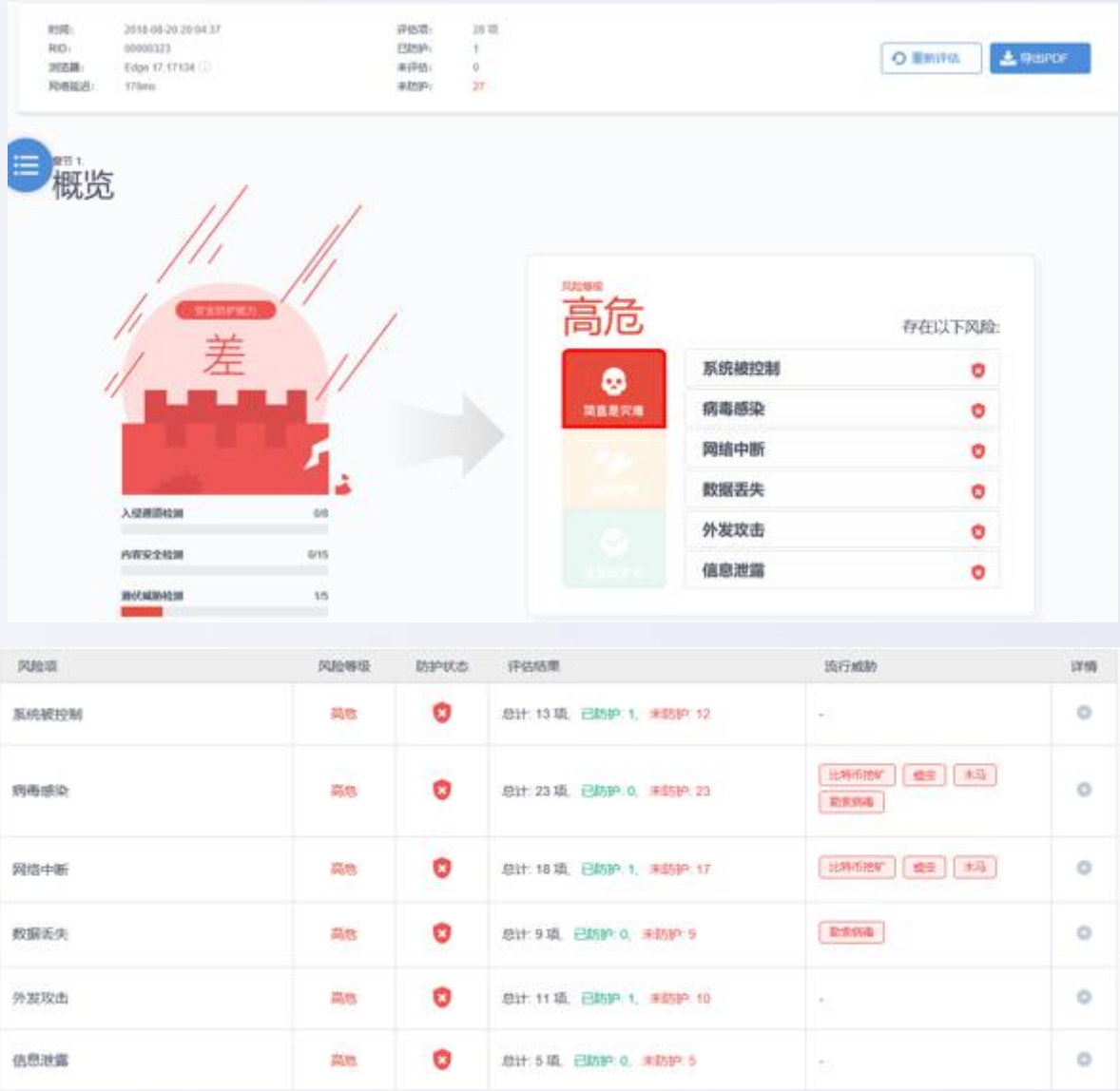
2、在评估器界面中，选中【已阅读并同意 服务条款 和 用户协议】，点击【开始评估】按钮后无需其他操作即可进入自动化评估流程。

注：在评估器界面中，首先需要使用用户名和密码并成功登陆才可使用，目前安全评估器只针对内部员工和渠道开放

1. 渠道使用深信服社区账号即可正常登陆；
2. 可以使用深信服员工的手机号作为用户名进行注册并登陆

2、产品推广工具—互联网有效性评估器

3、自动评估结束后，安全评估结果自动呈现。



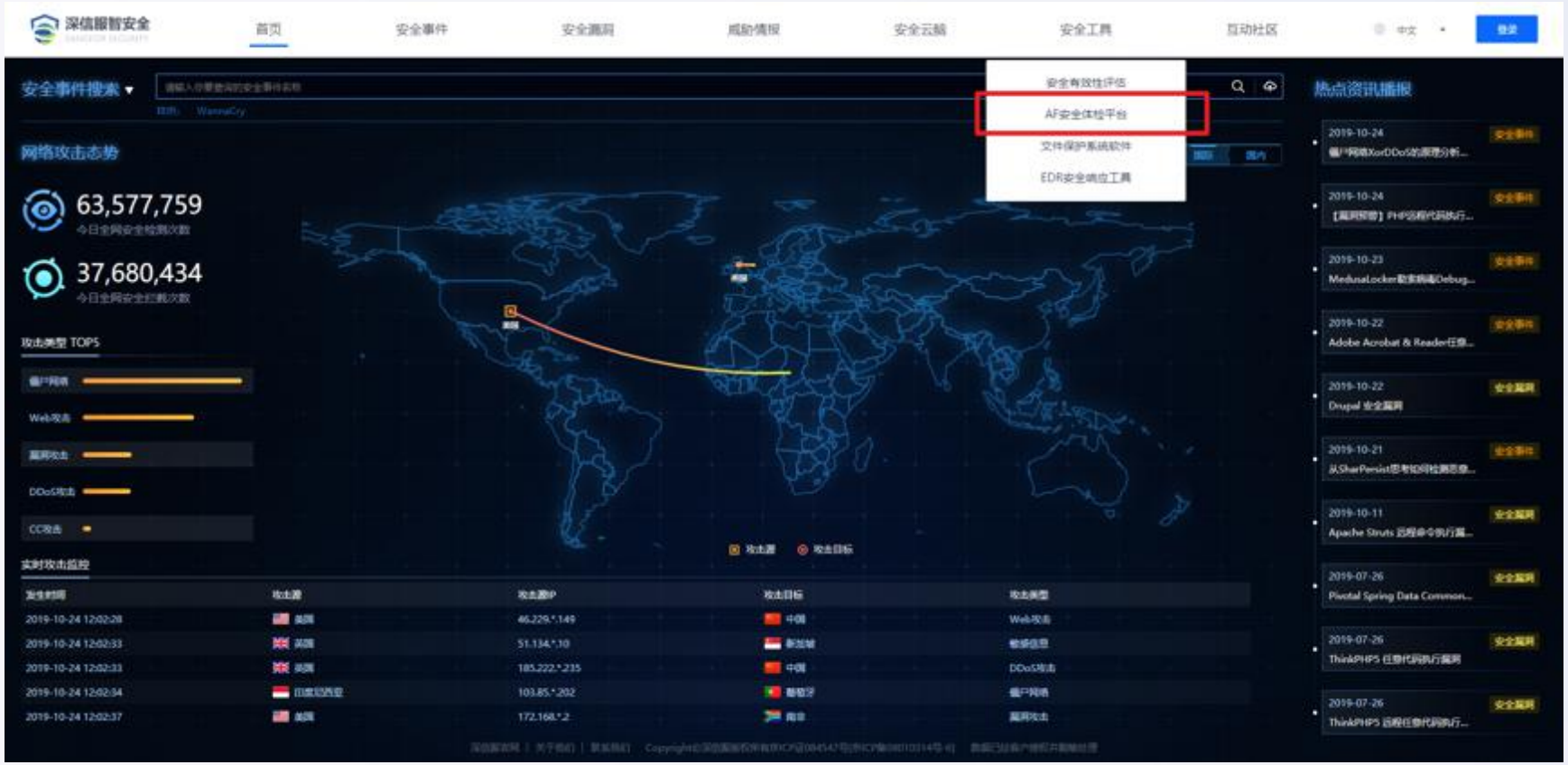
3、产品推广工具—安全体检平台

体检平台是什么

体检平台是一款根据部署在客户环境中的AF情况，云端交付可编辑的安全测试报告，极大的减少项目中制作测试汇报材料和日常巡检报告的工作量。

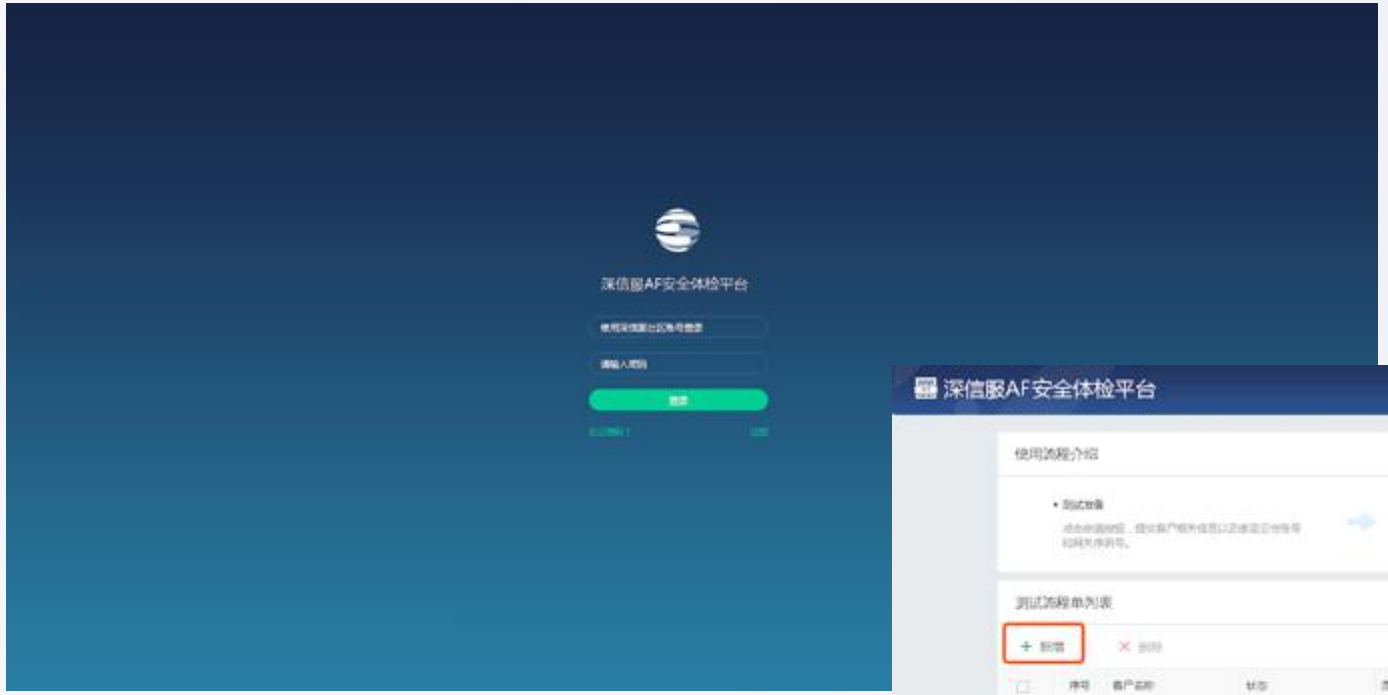
1.安全专家在线分析
2.专属报表直观展示
3.有效保障项目成功

① 登录网址：https://sec.sangfor.com.cn 选择【安全工具】-【AF安全体检平台】

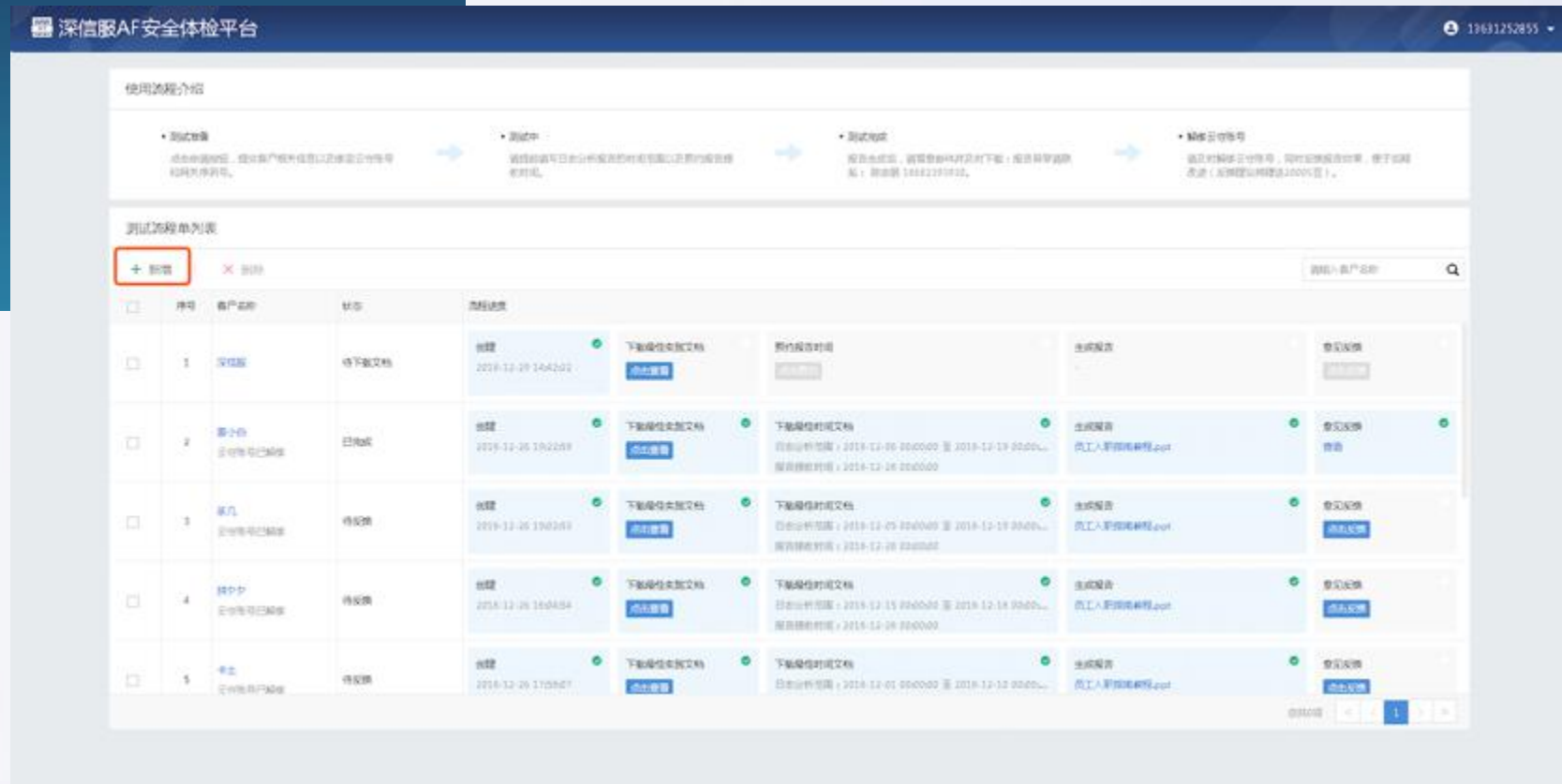


3、产品推广工具—安全体检平台

② 输入社区的账户密码，如果没有账户可以点击注册



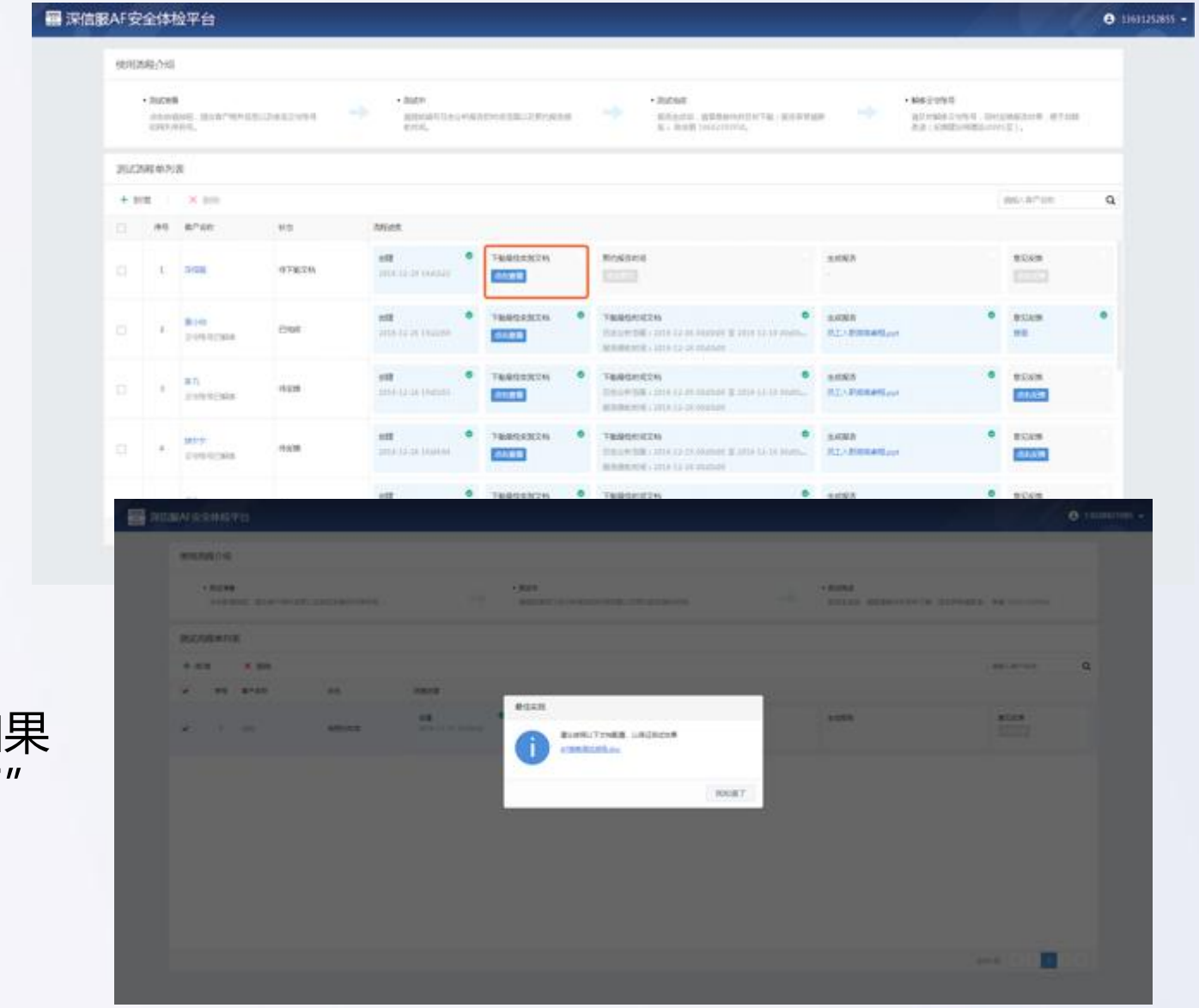
③点击新增按钮



3、产品推广工具—安全体检平台

④ 填写客户信息、网关序列号

⑤ 创建完成后，点击查看最佳实践文档



⑥ 点击文件即可下载，相关文件如果之前下载过直接点击“我知道了”即可

Microsoft Word 文档

4、产品推广工具—EMM演示平台

手机下载演示步骤：

1、浏览器输入：https://emm.safeapp.com.cn:12443/

2、下载安装aWork标准版，在手机通用-设备管理中选择信任证书

3、点击客户端，地址栏输入https://emm.safeapp.com.cn:12443/

4、输入账号sx123456，密码sx123456

5、产品推广工具—桌面云线上演示及测试平台

桌面云在线演示、测试平台:

http://adesklabs.sangfor.com.cn:8000/#/?_k=bmvrzz

THANK YOU

深信服科技股份有限公司