SANGFOR
深信服科技

融合媒体云安全运营体系的建设实践

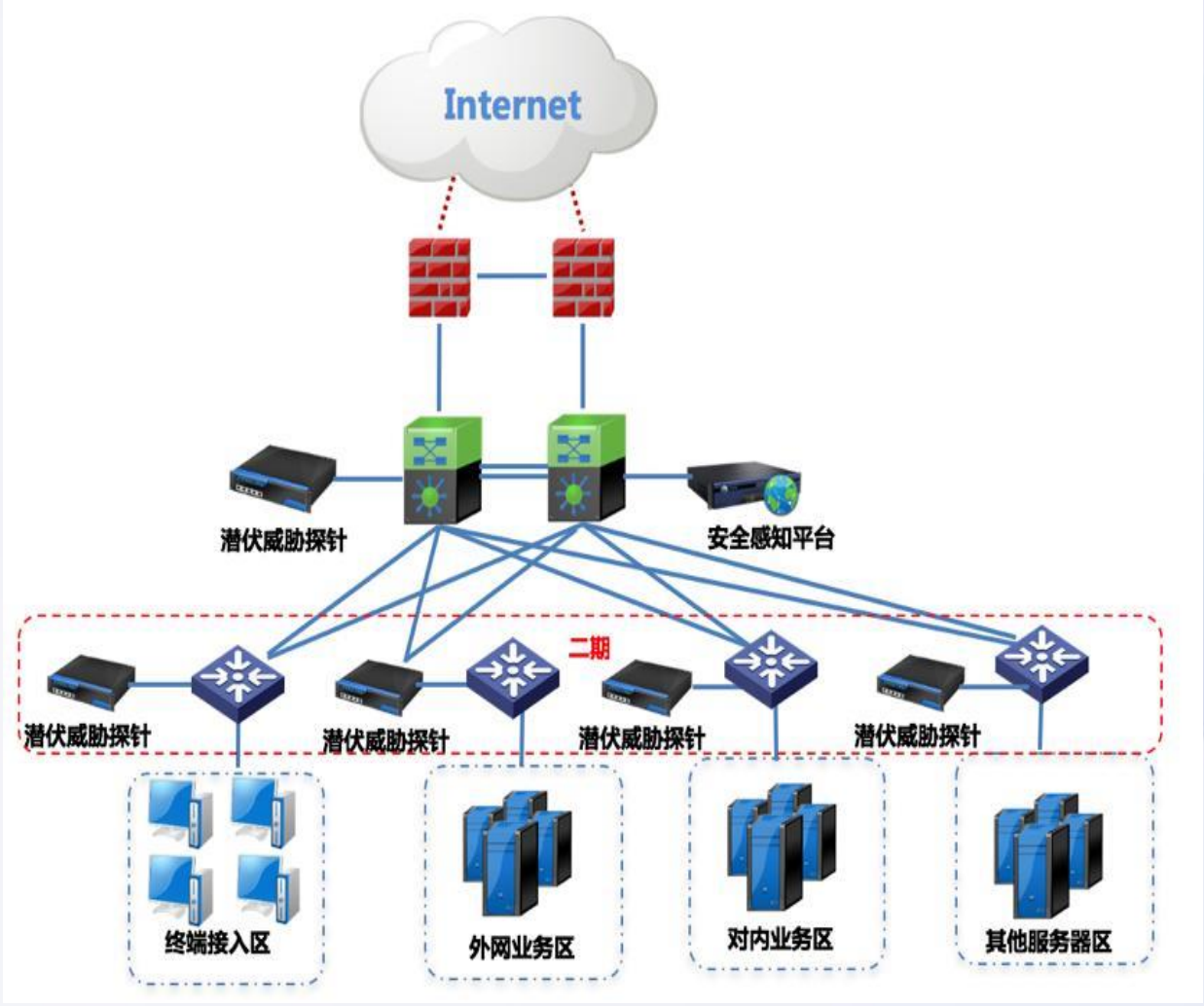
运营商事业部

广电总局信息中心

背景&部署方式

国家广电总局作为网信办14家部委态势感知试点单位之一，大力推进落实态势感知平台项目建设，恰逢十九大，广电总局信息中心发现内部服务器在无正常业务情况下，经常对境外地址发起主动访问。敏感时期，任何安全隐患都可能导致发生严重的安全事件 。

项目一期深信服为用户部署了1个分析平台、1个流量采集探针。平台和探针分别旁挂于核心交换机，在不影响用户现有网络结构的基础上，实现了对全网潜伏威胁的全面感知；项目二期计划在各个业务服务器区交换机和终端接入区交换机增加探针数量。



方案效果与价值

安全感知平台部署上去以后真正为用户发现了许多安全隐患，如弱口令、非法外连、内部横向攻击等等，尤其协助解决了用户最关心的非法境外外连的问题， 更为用户完善了整个安全体系。

全网安全风险可视：通过可视化的风险分析报表，将安全状态、资产情况、访问关系、行为、脆弱性等向用户进行直观的呈现，帮助安全管理人员快速实现了对全网安全状况的实时了解；

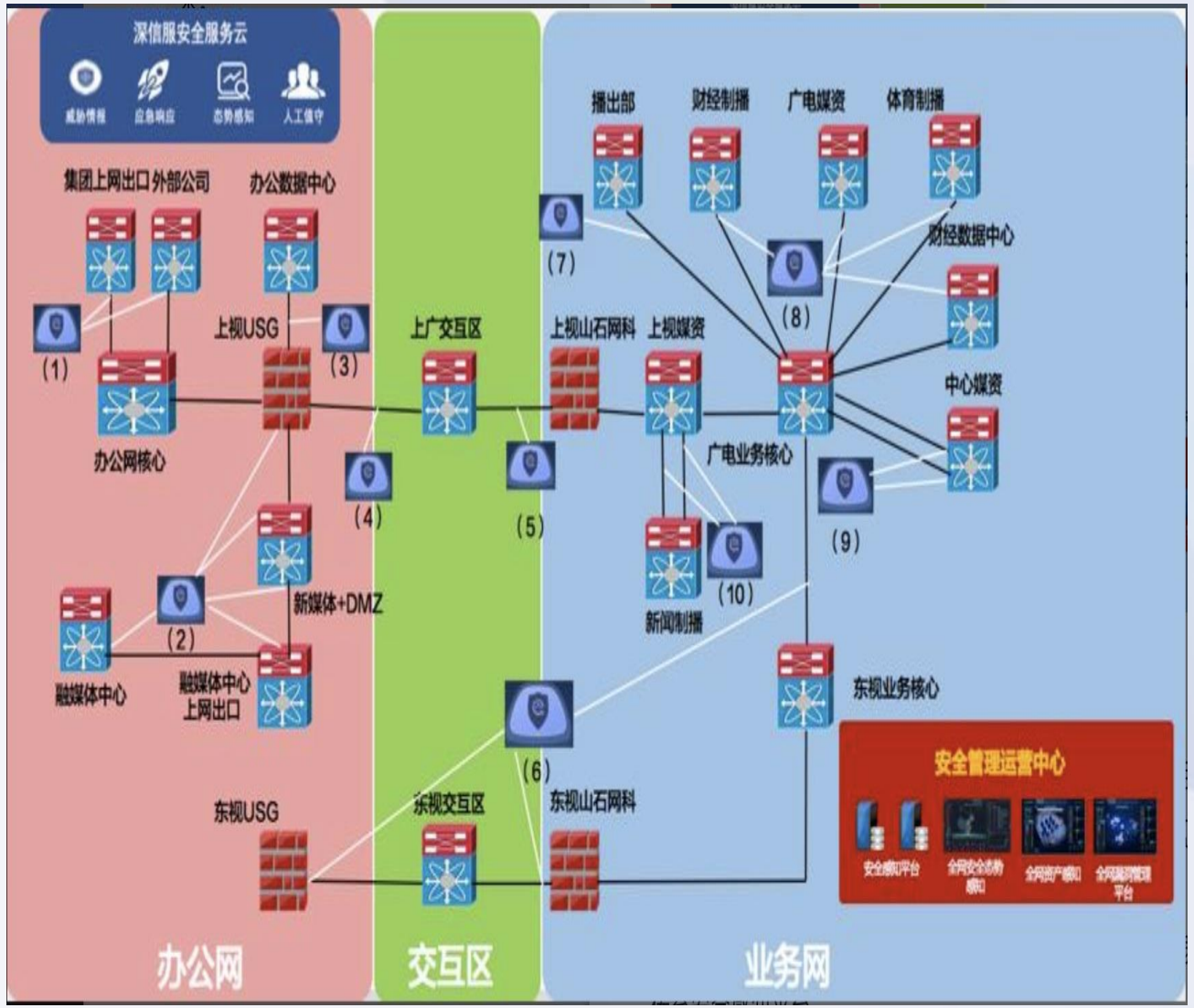
潜伏威胁的快速定位与发现：客户办公网内业务之间的访问路径、异常流量、存在异常行为的主机等进行可视化和预警，实现了对失陷主机、横向攻击等潜伏威胁的快速定位、快速发现，帮助管理员及时响应安全事件并进行安全策略调整；

上海文广集团

背景&部署方式

随着网络安全法、等保2.0等政策法规的相继出台，要求负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。在这种背景下，上海文广集团计划建设网络安全监测与预警平台。

办公网、交互区、业务网总共部署了13台探针，安全运维管理区部署了安全态势感知。



方案效果与价值

1.提升全网安全风险的监测预警能力

提升文广集团边界安全风险的监测能力、提升企业风险预警和快速响应能力、提升企业网络安全分析与管理能力。

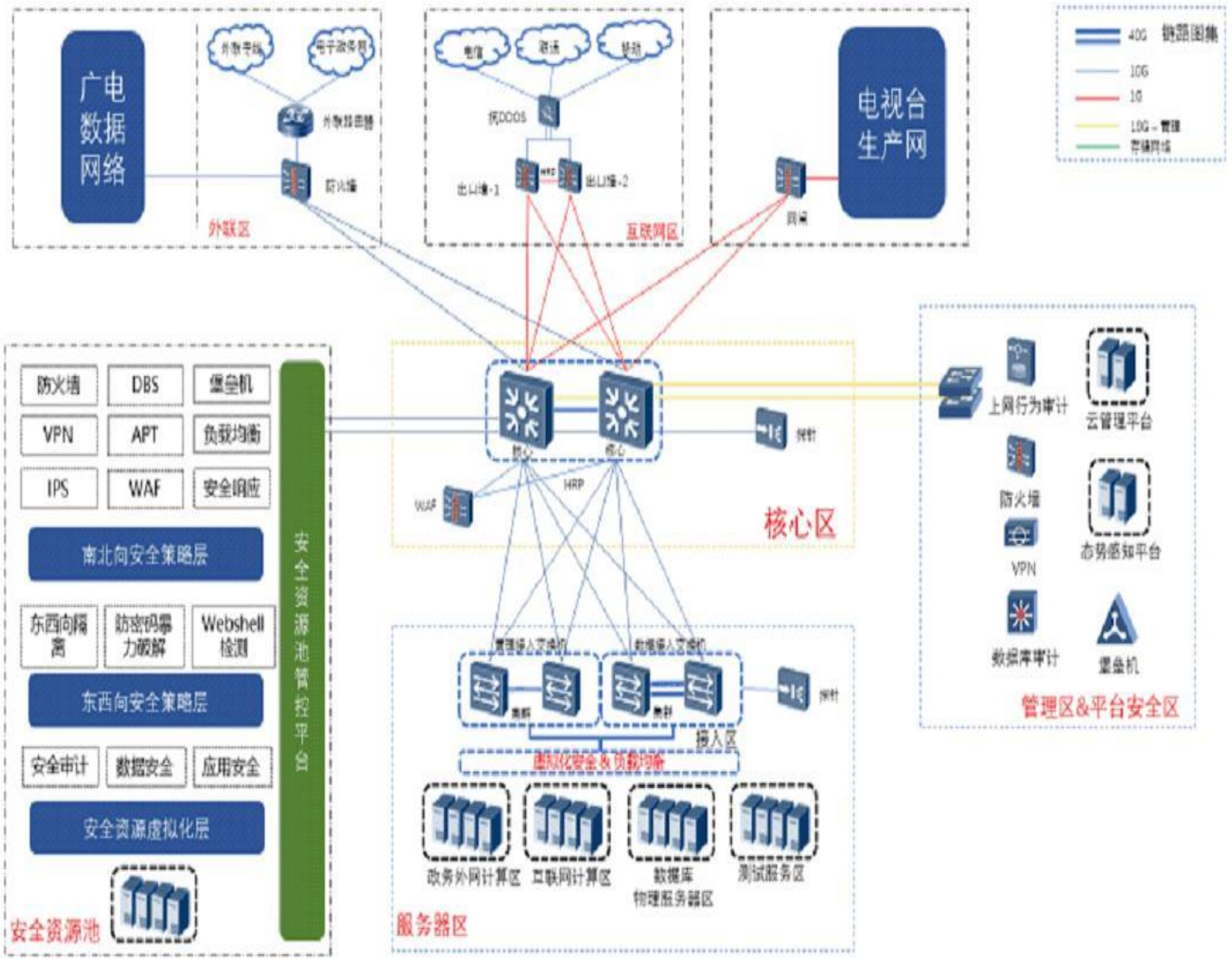
2.实现海量数据的安全价值挖掘，促进威胁发现能力提升；

通过推动监测预警技术持续研究，实现海量安全数据的集中运营，提升高密度、多关联性的安全价值挖掘能力。

3.构建立体化、系统化、智能化的运维管理体系；

针对广电业务进行更精准、更专业、更细致的数据分析，将网络安全监测预警的能力，紧密贴合融合媒体发展大趋势下的新型业务形态，实现跨业务、跨网络、跨平台、跨终端的立体化、系统化、智能化的运维管理体系。

恩施广电智慧云平台安全项目



项目背景

- **智慧广电云**：2018年恩施广电启动“智慧广电云”一期，推动广电核心业务平台上云，通过弹性计算、存储、网络资源为政企行业客户提供云服务；
- **等保合规**：依据《广播电视相关信息系统安全等级保护基本要求》满足云内、租户业务等保合规要求

安全核心需求

- **平台安全建设**：具备完整的安全防护能力，满足三级等保要求；
- **租户安全建设**：为租户提供相关的安全组件与服务，满足租户云上业务系统的等保合规要求；
- **安全管理建设**：构建一个运营管理中心，具备平台、租户等业务系统的未知威胁检测和安全管理能力，可为租户提供运营报告、威胁监测报告等增值服务。

深信服解决之道

- **边界安全**：安全域边界部署防火墙/网闸，数据中心部署WAF、安全资源池和EDR，构建多级安全防御体系，满足云平台、云边界/租户、云主机等多级隔离需求；
- **软件定义安全**：安全资源虚拟，构建一个云上安全市场。为租户提供下一代防火墙、终端安全EDR、VPN、DAS、行为管理、负载均衡等安全组件服务；
- **安全大脑**：通过部署安全感知平台+潜伏威胁探针，实现全流量安全检测，统一呈现安全威胁、安全态势；

融合媒体大趋势下广电业务架构发生了变化

SANGFOR 深信服科技

泛网络


有线卫星


互联网


IPTV

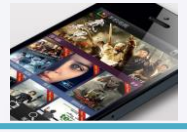
4K

泛终端


IPAD


电视


电脑


手机

新平台


广电云


融媒体


OTT


大数据

新安全


网络安全法


等保2.0


勒索病毒


云安全

- ✓ 媒体融合的浪潮下，内容从汇聚、生产、管理再到分发正全流程融合重构；
- ✓ 打造报、台、网、微、端的多元化传播，提高新闻舆论传播力、引导力、影响力、公信力；
- ✓ 新法规、新安全、云安全是保障广电行业关键基础信息设施保障新方向；

安全形势快速变化

2008年
我们在谈的网络安全

2019年
我们在谈的网络安全

未来

广电行业面临全新的安全挑战

互联网+与云计算技术，导致边界发生变化

暴露面越来越多

隐蔽性越来越强

加密传输、隐蔽信道、代码混淆

安全挑战

攻击程序自动化，恶意程序工程化

攻击越来越频繁

敏感资源越来越集中

广电业务深度融合，攻击目标价值扩大

对抗的要求---我们是否能够“持续性的防护、检测、响应，并能提前分析预警”

只有面向未来，才能有效保护

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

PDR

技术因素 → 智能 → 智能进化

人的因素 → 运营 → 以人为本

法国人
战死2000多人
统帅内穆尔被枪杀

西班牙人
贡萨洛运用火枪
战死不到500人

“火药把整个骑士阶层炸得粉碎”
——马克思

切里尼奥拉战役告诉我们，击败骑士的不是更强的骑士，而是你不认识的武器。攻防需要面向未来，才能形成有效的保护。

面向未来保护的架构体系

自动化智能监测，有效检测未知威胁

全局安全可视

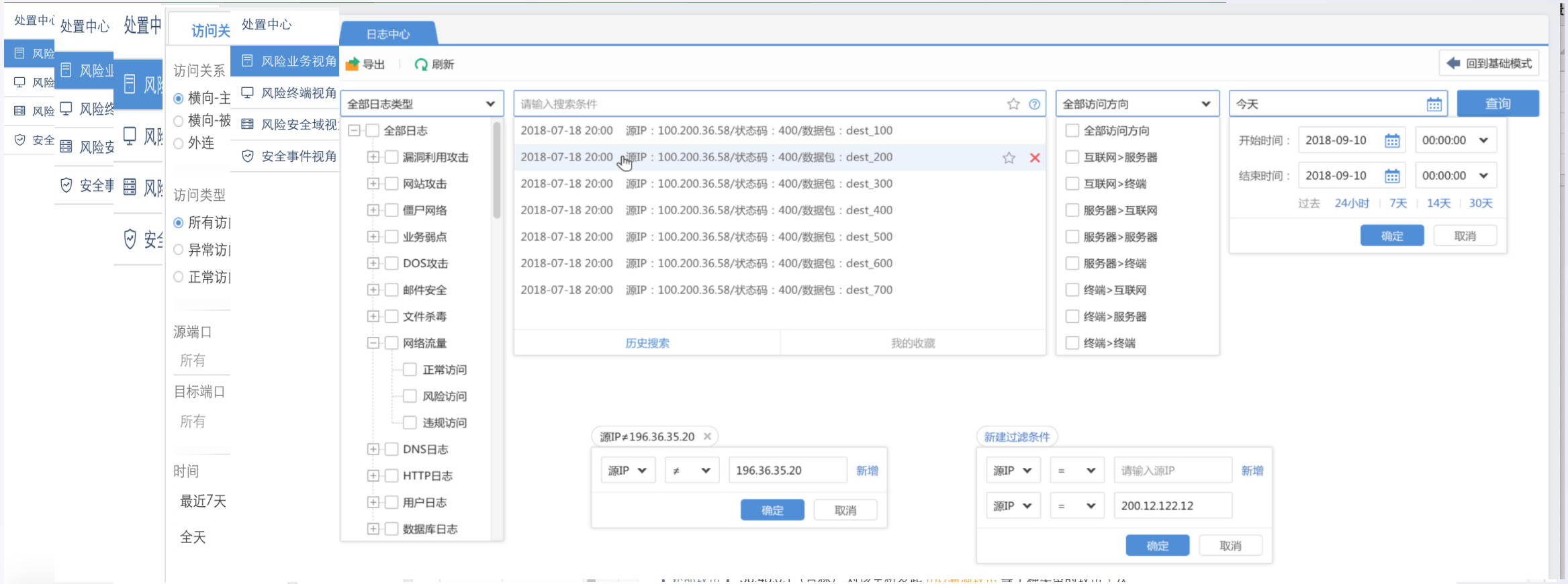
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

全网安全态势可视 → 外部攻击态势可视 → 横向攻击态势可视 → 业务外连风险可视 → 业务脆弱性与风险可视

高效运维分析

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

业务维度可视 → 攻击链可视 → 事件举证 → 影响面分析 → 攻击入口点溯源 → 元数据溯源



安全应急运维处理中心

安全运营中心发现病毒 → 中心发起处置工单 → 专家在线审核，指派处理团队 → 指挥中心统一调度，协助问题处理 → 问题复核，事件归档

资产风险安全运维管理中心

多产品统一管理

- 对深信服所有的网络安全设备(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

告警推送

- 安全风险事件告警、VPN网络告警、分支离线、授权告警、资源告警等

分支设备统一管理

- 安全设备配置统一下发
- 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

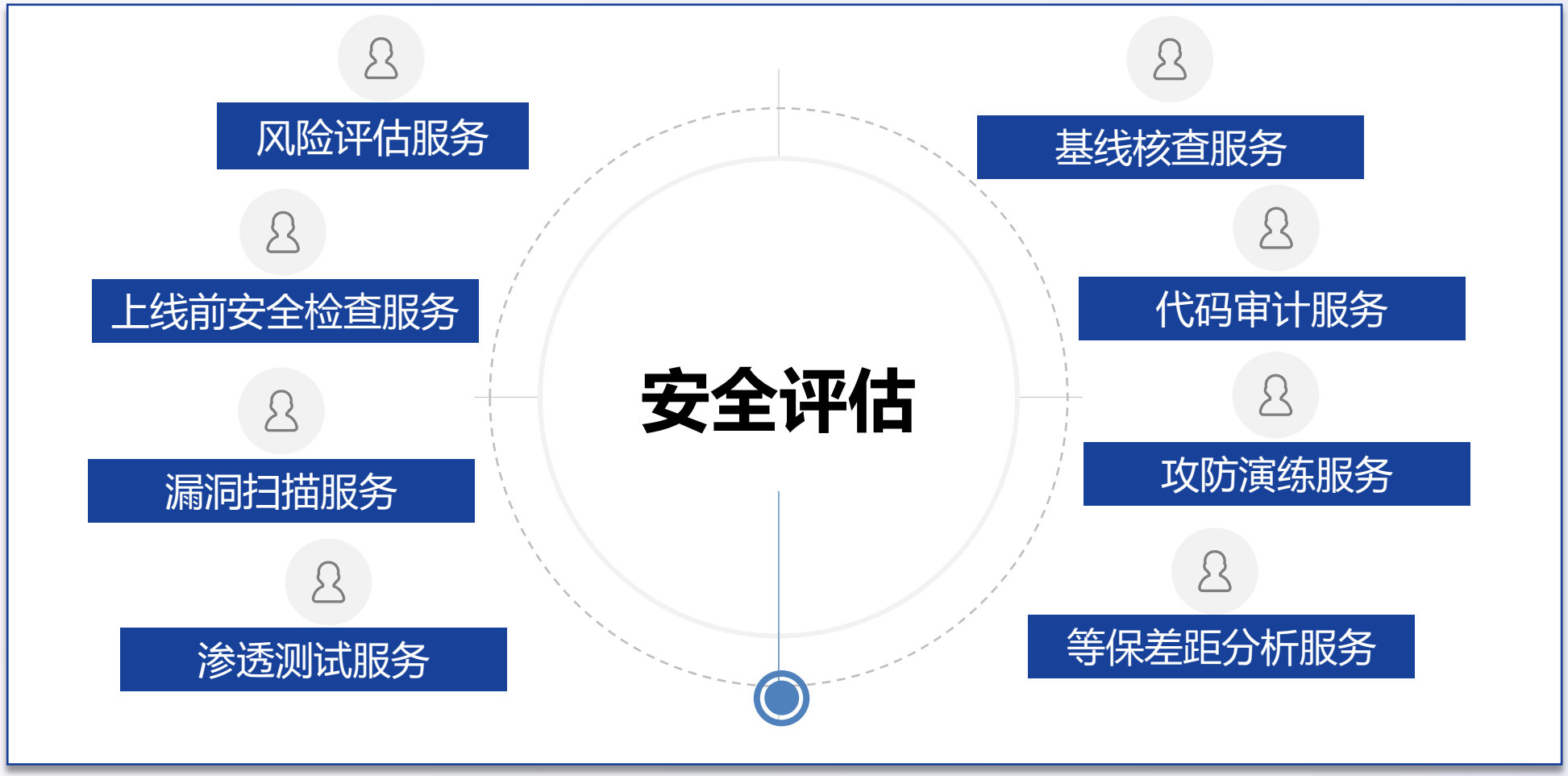
集中查看和处置安全风险

- 收集安全设备/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

周期性安全评估，提前洞悉风险



通过外部专家评估的方式验证现有安全体系健壮性，提前**洞悉风险，规划未来！**

SANGFOR
深信服科技

THANK YOU