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

企业信息安全建设规划解决方案

深信服 智安全

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

一．信息安全现状与挑战

二．深信服的理解与建议

三．我们提供的解决方案

四．技术能力与客户案例

数字化时代威胁升级

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

攻击频发

勒索病毒、数据泄露、黑客入侵等网络安全事件呈现上升趋势

来源：互联网

数字化时代威胁升级

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

2017年TOP威胁	2017年评估趋势	2018年TOP威胁	2018年评估趋势	排名变动
1.恶意软件	→	1.恶意软件	→	→
2.基于Web的攻击	↑	2.基于Web的攻击	↑	→
3.Web应用程序攻击	↑	3.Web应用程序攻击	→	→
4.网络钓鱼	↑	4.网络钓鱼	↑	→
5.垃圾邮件	↑	5.拒绝服务	↑	↑
6.拒绝服务	↑	6.垃圾邮件	→	↓
7.勒索软件	↑	7.僵尸网络	↑	↑
8.僵尸网络	↑	8.资料外泄	↑	↑
9.内部威胁	→	9.内部威胁	↓	→
10.物理操作/损坏/盗窃/损失	→	10.物理操作/损坏/盗窃/丢失	→	→
11.资料外泄	↑	11.信息泄露	↑	↑
12.身份窃取	↑	12.身份窃取	↑	→
13.信息泄露	↑	13.加密劫持	↑	新增
14.漏洞利用套件	↓	14.勒索软件	↓	↓
15.网络间谍活动	↑	15.网络间谍活动	↓	→

Source From 《ENISA Threat Landscape Report 2018——15 Top Cyberthreats and Trends》， ENISA 2019

网络安全监管标准愈发严苛

网络安全法规政策

2016.11
中华人民共和国全国人民代表大会高票通过《网络安全法》

2016.12
经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》

2017.05
国家互联网信息办公室发布《网络产品和服务安全审查办法（试行）》

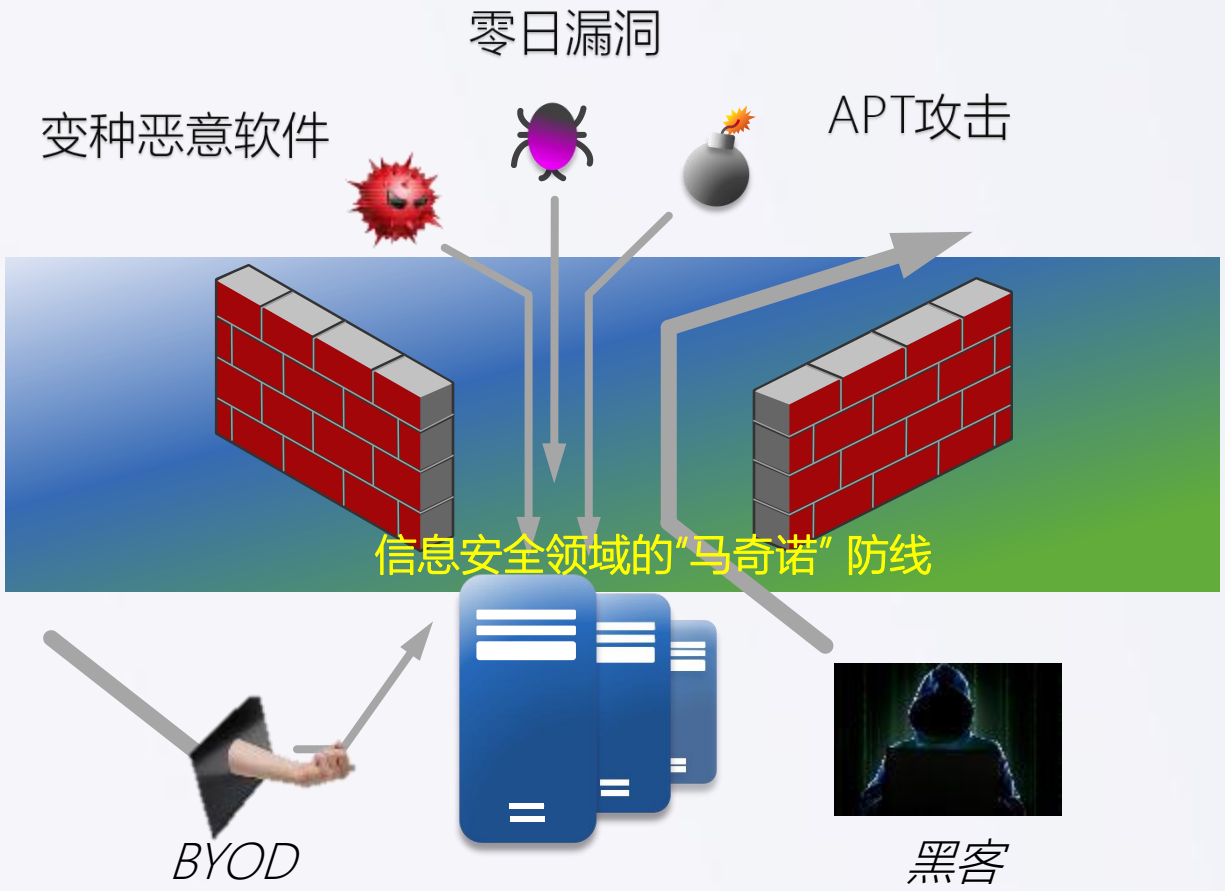
2017.06
《网络安全法》正式生效

2017.07
各行业开展业务系统网络安全检查

2019.05
《信息安全技术网络安全等级保护基本要求》等三大核心标准发布

2019.05
国家互联网信息办公室会同相关部门研究起草《数据安全管理办法（征求意见稿）》

传统安全防护逐步失效



传统防火墙、IPS、杀毒软件等基于特征库的安全检测，无法过滤：

变种僵/木/蠕

U盘带入

恶意的内部用户

BYOD带入

零日漏洞

APT攻击

“世界上只有两种人，一种是知道自己被黑了的，另外一种是被黑了还不知道的。”

——美国前国土资源部部长

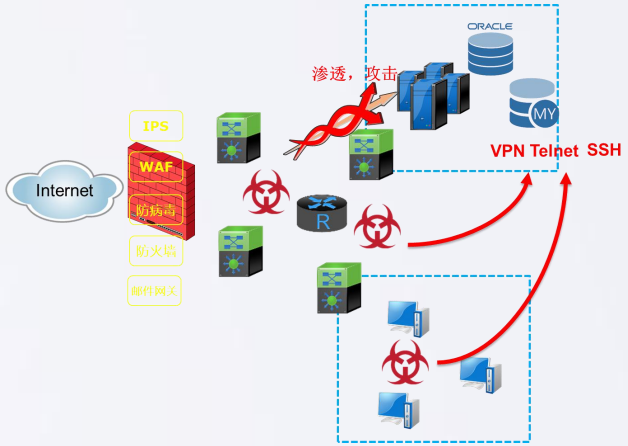
安全风险能见度不足

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

看不清资产

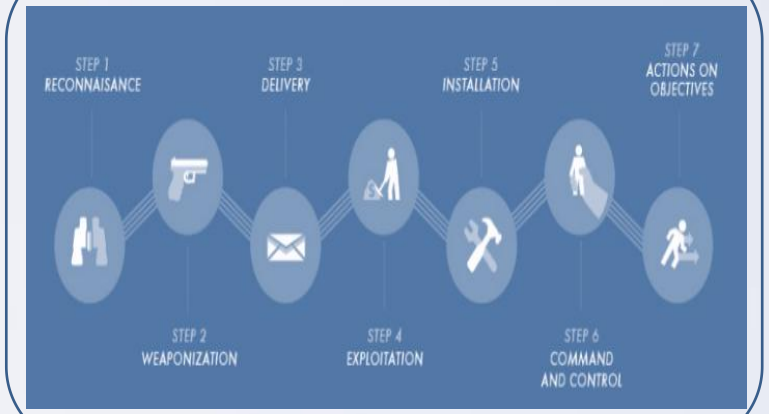
- 看不清的新增资产产生安全洼地
- 缺乏有效手段主动识别新增业务
- 攻击者对内网未被归档和防护的新增资产进行攻击，顺利渗透如内网。

看不见新型威胁



- 水坑攻击
- 鱼叉邮件攻击
- 零日漏洞攻击
- 其他攻击

看不见内网潜藏风险

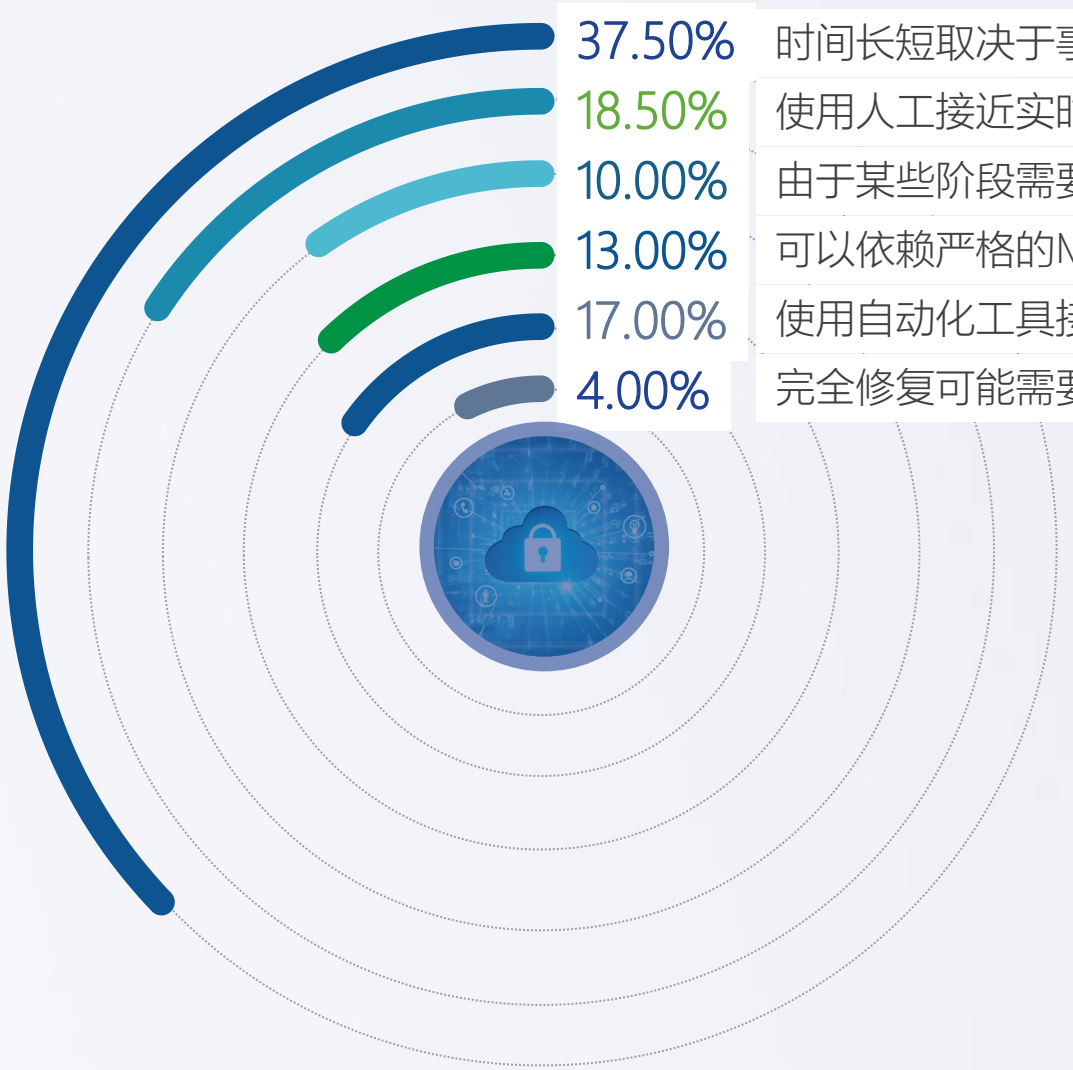


- 黑客内部潜伏后预留的后门
- 伪装合法用户的违规操作行为
- 封装在正常协议中的异常数据外发
- 看不见的内部人员违规操作

缺乏自动化防御手段

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

企业普遍缺乏
自动化防御手段



37.50%	时间长短取决于事件本身
18.50%	使用人工接近实时处理
10.00%	由于某些阶段需要人工操作，需要花费数周时间
13.00%	可以依赖严格的MSSP SLA
17.00%	使用自动化工具接近实时处理
4.00%	完全修复可能需要数月，包括调查在内

来源：IDC报告

企业信息安全建设规划目标

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

风险可视化（Visibility）

未知攻，焉知防，看见风险才能防范风险

防御主动化（Proactive）

最好的防守是进攻，主动防御，纵深防御是设计的目标

运行自动化（ Automation ）

全天候自动化的安全运营才能保障安全体系的落实

安全智能化（Intelligent）

信息安全未来的重点将转向智能驱动，并能抵御未知高级威胁

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

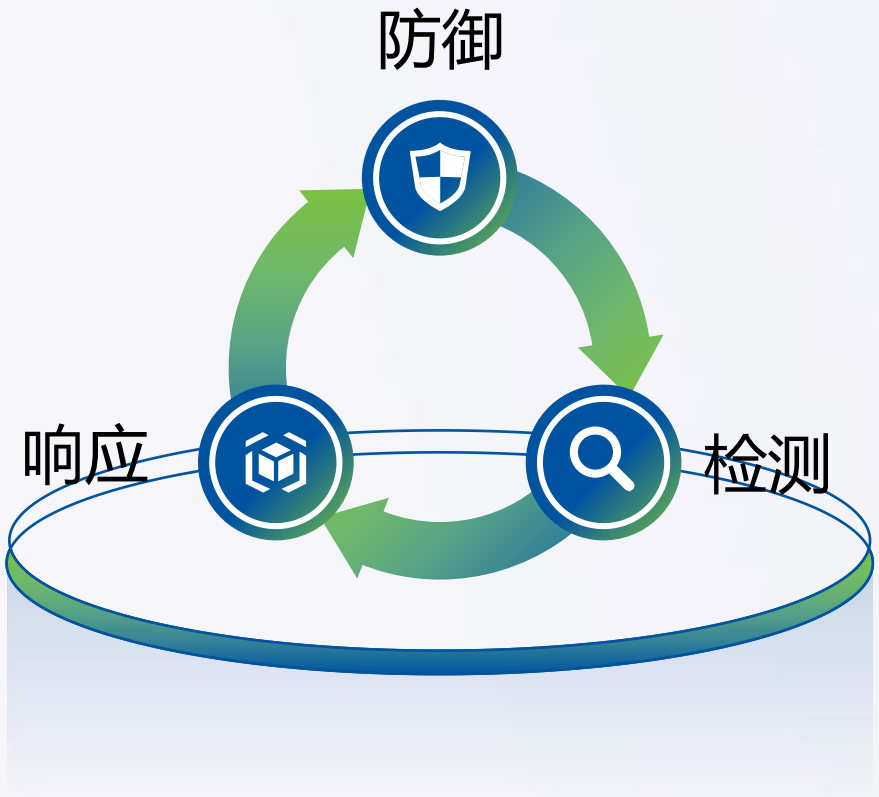
一．信息安全现状与挑战

二．深信服的理解与建议

三．我们提供的解决方案

四．技术能力与客户案例

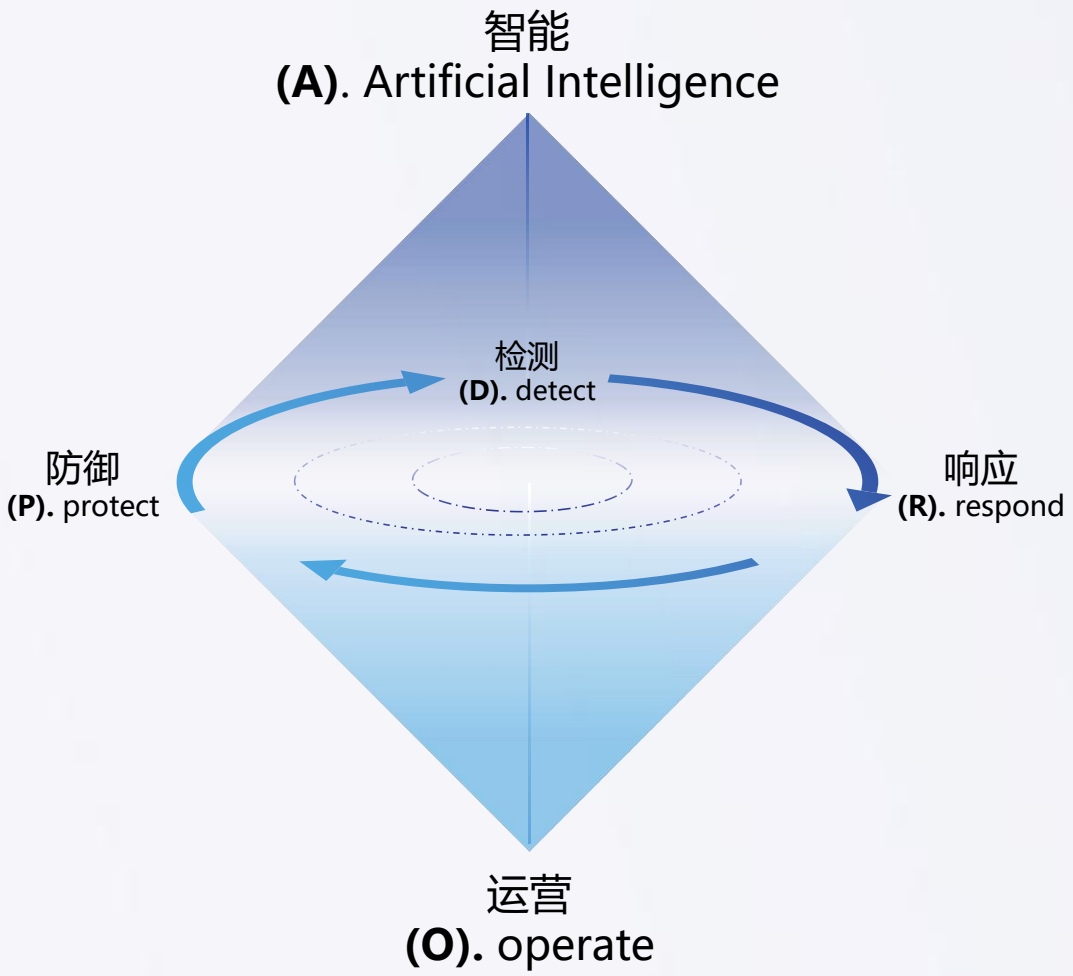
网络安全行业对风险的应对



ISO27001

信息安全管理体系

深信服APDRO智安全架构



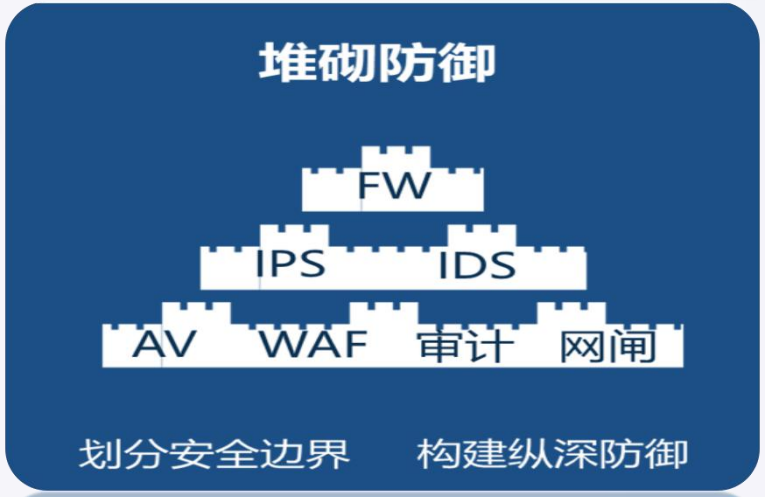
智安全能力模型

- PDR：从防御能力向检测和响应能力增强
- 智能：提升自动化能力应对大量未知威胁
- 运营：让安全产品用起来、管理制度落地

传统安全方案痛点

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

特点一：产品堆叠为主

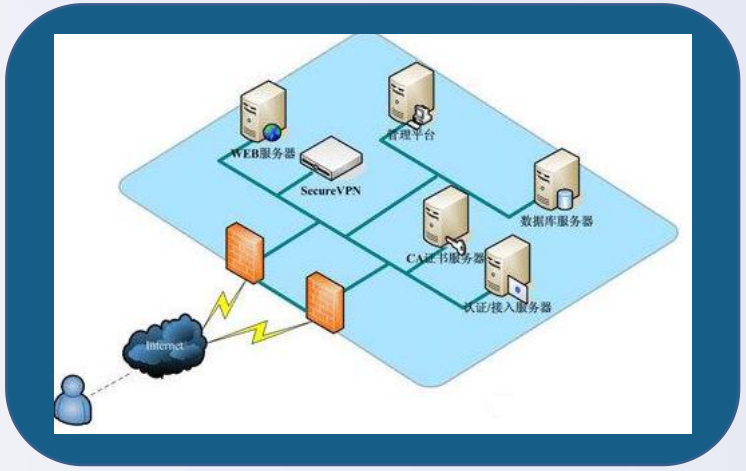


- 基于产品堆叠的安全建设方式，导致设备之间缺乏联动、安全运维负责

特点二：边界防护为主

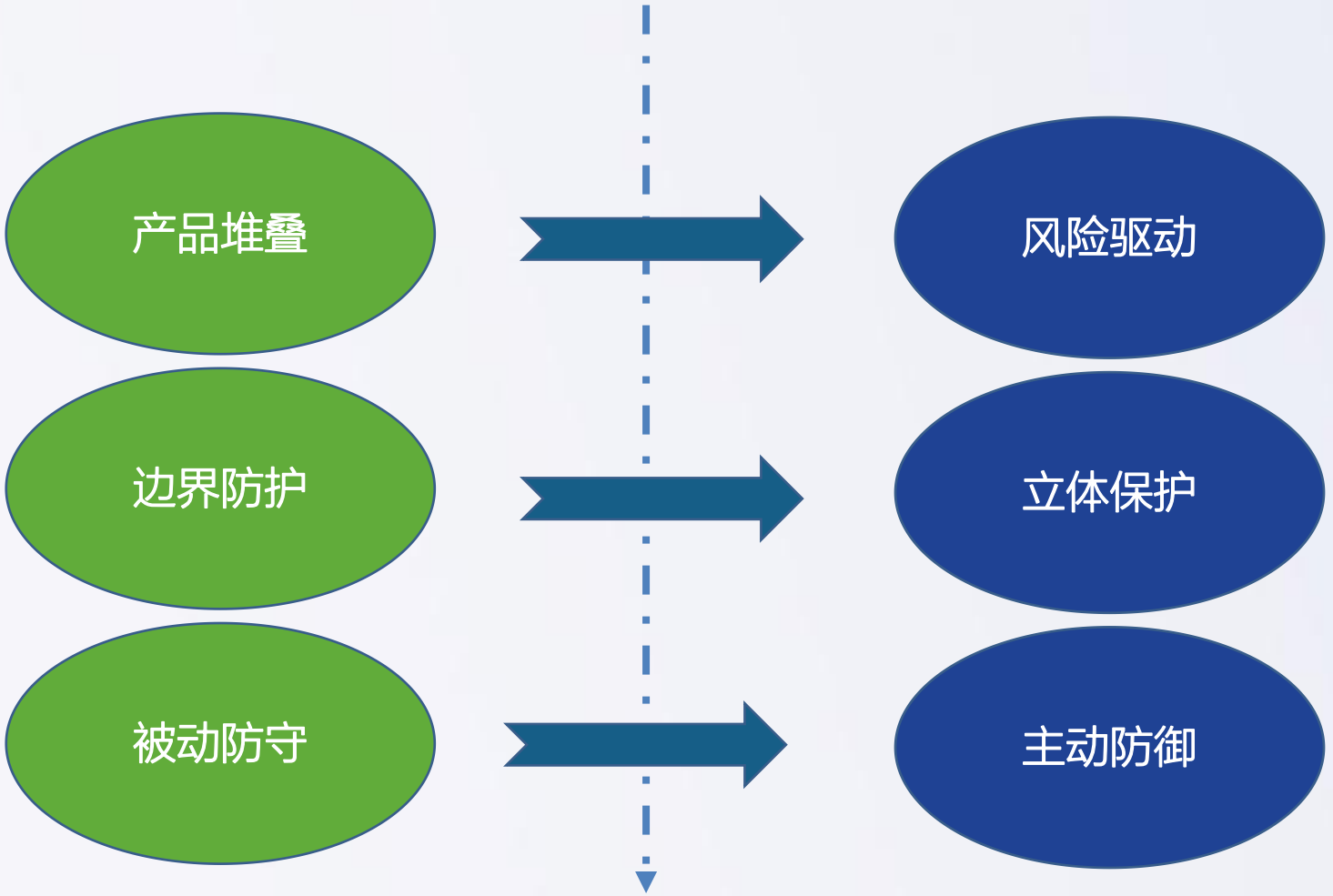
- 单纯边界防护为基础的解决方案，一旦边界被突破内网一马平川

特点三：被动防守为主



- 依靠挖掘漏洞、匹配特征、设置规则的被动防御模式，缺乏威胁情报，导致不能有效防护新型新型

深信服安全建设思路



过去的安全建设

现在的安全建设

风险驱动：安全需要“对症下药”

评估风险		处置风险
边界防护 ✓	→	现有防火墙、WAF、IPS保持策略开启
传统杀毒 ✓	→	具备传统杀毒能力，但无法应对勒索病毒、挖矿等
安全漏洞 ✗	→	安全漏洞大量未修复，且包含高危漏洞，需要尽快修复。
新型威胁 ✗	→	APT攻击、0 Day、社工等新型威胁不能防范，建议新增设备
合规要求 ✗	→	等保2.0、网络安全大检查部分不满足，建议新增设备

立体保护：网端云智能协同安全

云端实时赋能
持续增强网端能力

云

网端联动
云端赋能

加强身份认证、L2-L7层边界防护、未知威胁检测能力

网

端

完整的终端保护，防止外部威胁入侵，保障计算环境可信安全

加强风险评估、安全加固及应急响应服务，弥补自动响应不足

主动防御：基于威胁情报，提前锁定“敌情”

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

深信服
安全设备

厂商
安全情报

全网
安全信息

威胁情报采集

安全云脑

- 高可用架构
- 海量数据汇聚
- 大数据分析与挖掘
- 多引擎综合判定
- 智能安全分析

威胁情报
漏洞情报
情报信誉
文件信誉
URL信誉
域名信誉
文件云查
云查杀
URL云查
域名云查
僵尸网络
病毒
Web攻击
规则模型
APT
Web shell
未知攻击
安全风险
威胁分析
攻击回溯
黑客画像

基于AI、大数据技术，持续赋能

安全能力持续输出

全球威胁5分钟协同响应
全球热点事件1小时响应
安全能力高频更新

响应速度变快

安全设备能力增强

形成主动防御能力

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

一．信息安全现状与挑战

二．深信服的理解与建议

三．我们提供的解决方案

四．技术能力与客户案例

企业级安全体系整体框架

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

网端云协同新一代安全架构

风险驱动 立体保护 主动防御

技术

云：威胁情报 SAAS化服务 云端监测 在线专家

网： 边界安全 通信安全 接入安全 身份安全 安全大脑

端：主机安全 应用和数据安全 移动安全 IOT设备安全

管理

管理制度

管理机构

管理人员

建设管理

运维管理

运营

安全评估

资产管理

漏洞管理

威胁检测预警

威胁主动响应

事件应急处置

攻防演练

智能

智能流量分析 智能文件分析 日志关联分析 安全数据基线 安全云脑 威胁情报 机器学习

防御

网络防御 应用防御 零信任

检测

已知威胁 未知威胁 安全监测

响应

应急预案 应急演练 事件分析

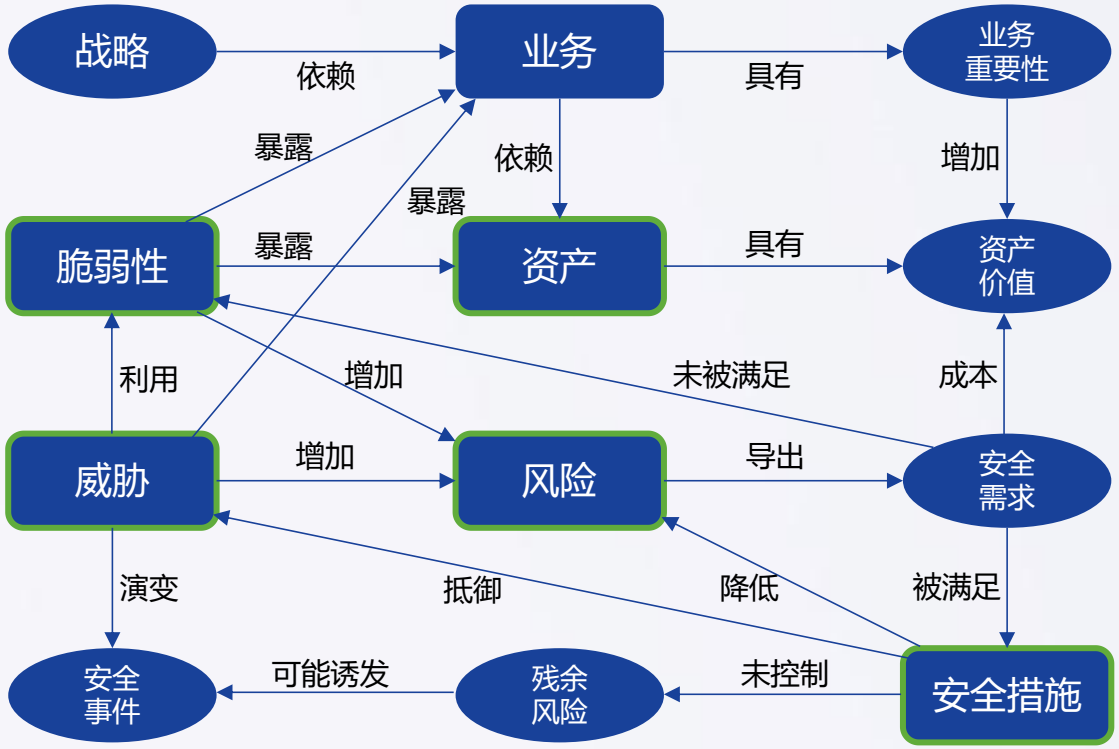
运营

安全治理 管理策略 风险评估 风险处置 资产管理 供应链风险管理 业务连续性管理

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

一、风险驱动的安全闭环能力

风险管理简介



风险评估要素关系图
GB/T 20984 信息安全技术 信息安全风险评估规范
（本稿完成日期：2018年1月）

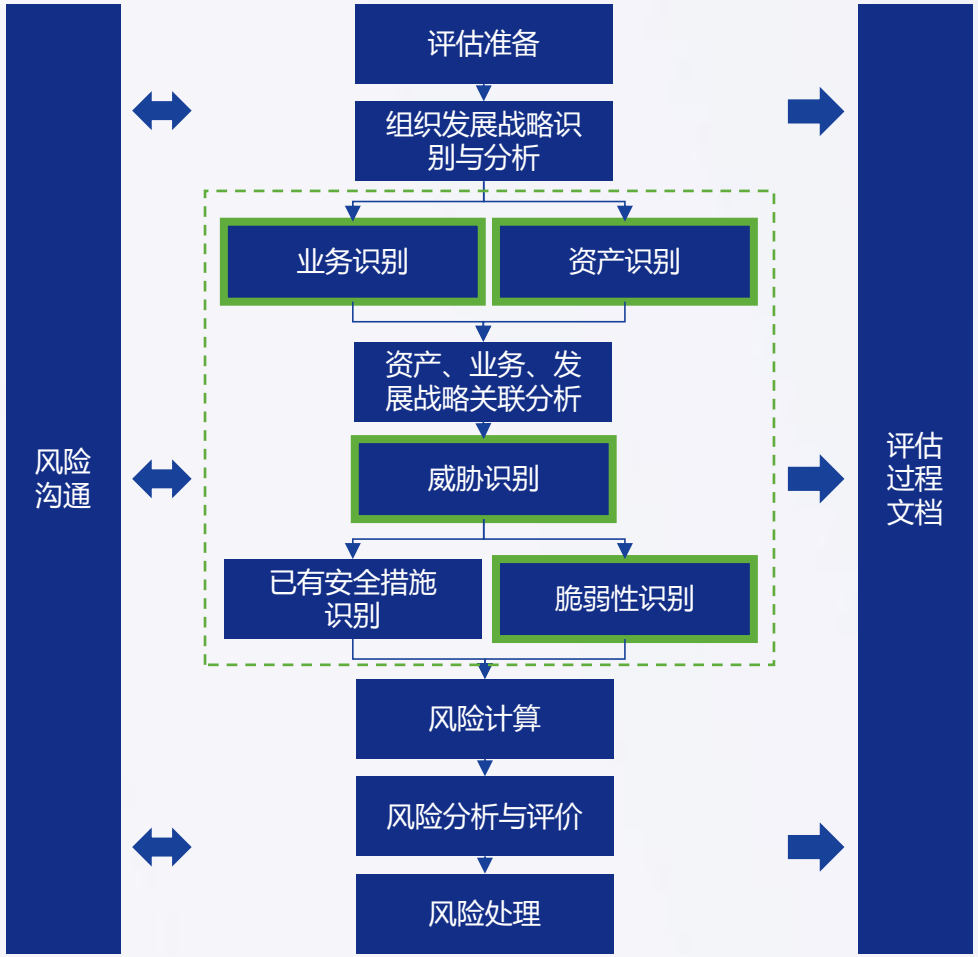
网络安全风险：关于目标的负面**影响**的**可能性。**
网络安全风险=（影响，可能性）=（资产，脆弱性，威胁）

过去常用的风险管理模型有：**PDR**（防御、检测和响应）、**PPDR**（安全策略、防御、检测和响应）、**ASA**自适应安全框架（预测、防御、检测、响应）、**PDRR**（防御、检测、响应和恢复）、**MPDRR**（管理、防御、检测、响应和恢复）和**WPDRRC**（预警、防御、检测、响应、恢复、反击）等动态安全模型。

常用的风险控制措施集包括：《网络安全等级保护基本要求》、《信息安全管理体系要求》（ISO27001 附录A）等。

PDR的闭环安全体系已经得到大多数企业的认可，成为网络安全风险管理模型的最佳实践。

第一步：风险评估



GB/T20984 风险评估流程

风险评估有上百种方法，安全扫描、专家判断、历史事件分析、控制措施检查、德尔菲法、SIP测试、头脑风暴，GBT20984只是风险评估的一种。不论哪种风险评估方法，资产、威胁、脆弱性都是重要因素。

由风险管理高级执行层监督指导，由业务/流程层执行

数字化转型　智慧XX　云计算　移动互联网　物联网　大数据

资产识别：常见业务和资产

钓鱼、鱼叉式钓鱼
隐蔽下载、水坑攻击、恶意广告
代码注入、Webshell
键盘记录、会话劫持
Hash传递攻击、Ticket传递攻击
窃取凭证
网关破坏
恶意软件
DDoS
定向狙击
身份窃取
商业间谍
交易劫持
银行账号窃取
勒索
企业公众号窃取、企业DNS劫持
中间人劫持
企业高层定向狙击
蓄意攻击
IT封锁
横向渗透
IT破坏
宕机
声誉破坏
网页篡改
注意力转移、声东击西
阶段性破坏

威胁识别：27种常见的攻击向量

未初始化指针访问
算法复杂性
无限制的句柄分配
参数注入或修改
不对称资源消耗
身份验证不当
缓冲区错误
信道和路径错误
清理错误
代码开发设计实现错误
代码注入
命令注入
配置错误
容器错误
凭证管理不当
跨站请求伪造
跨站脚本攻击
加密问题
数据处理不当
数据反序列化不当
除零问题
两次释放
编码错误
环境问题
威胁函数暴露
不当的资源暴露
文件和目录信息曝光
授权不当
访问控制不当
加密力度不足
密钥管理不当
……

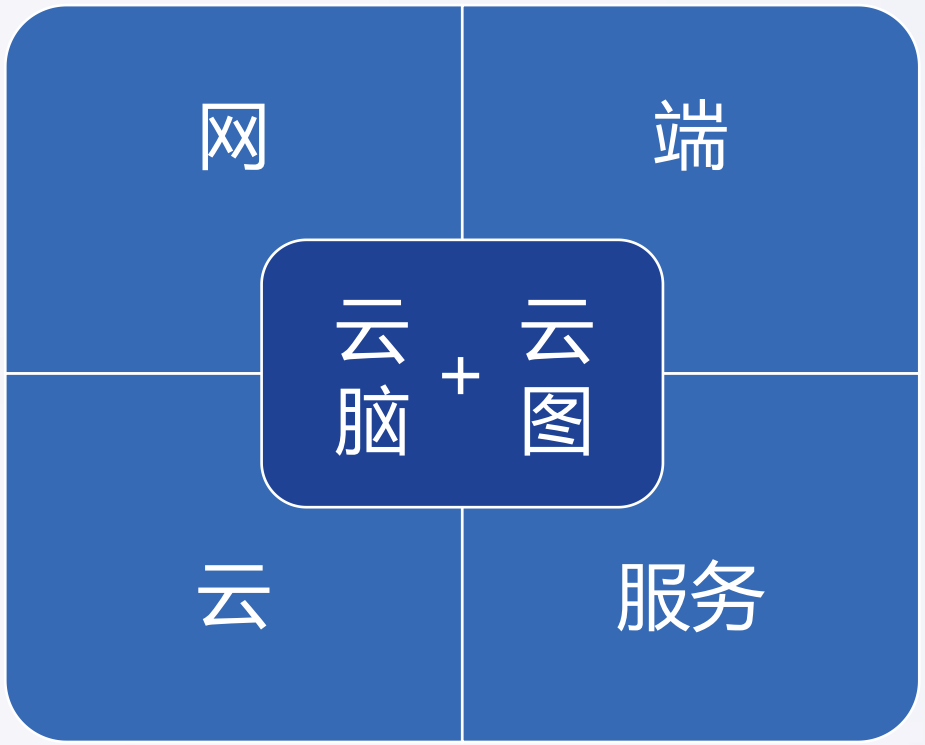
脆弱性识别：NVD CWE常见脆弱性列表
https://nvd.nist.gov/vuln/categories

第二步：风险处置-确定风险控制措施

功能域	风险控制措施子集
智能	智能流量分析（AI.NW）：对网络中的流量，以及流量中各协议栈内容进行提取，进而实现智能化分析，发现其中的恶意流量。
	智能文件分析（AI.FL）：对各类文件进行智能分析，发现其中的恶意文件，文件类别包括但不限于PE、DOC、PDF、Shell等。
	日志关联分析（AI.RA）：对企业内安全设备和关键系统的日志进行关联分析，从全局的角度发现安全事件。
	数据基线（AI.BL）：对企业内各类数据进行基线建模，以发现异常行为。
防御	身份认证和访问控制（PR.AC）：对物理和逻辑资产及相关设施的访问仅限于授权用户，流程和设备，并且与未经授权访问授权活动和交易的评估风险一致地进行管理。
	数据安全（PR.DS）：管理信息和记录（数据）与组织的风险策略一致，以保护信息的机密性，完整性和可用性。
	信息保护流程和程序（PR.IP）：维护安全策略（解决组织实体之间的目的，范围，角色，责任，管理承诺和协调），流程和程序，并用于管理信息系统和资产的保护。
	防御技术（PR.PT）：提供对攻击的防御能力，以确保系统和资产的安全性和弹性，符合相关政策，程序和协议。
检测	异常和事件（DE.AE）：检测到异常活动并理解事件的潜在影响。
	安全持续监控（DE.CM）：监控信息系统和资产，以识别网络安全事件并验证保护措施的有效性。
	检测过程（DE.DP）：维护和测试检测过程和程序，以确保对异常事件的认识。
响应	响应计划（RS.RP）：执行和维护响应流程和过程，以确保响应检测到的网络安全事件。
	通信（RS.CO）：响应活动与内部和外部利益相关者协调（例如执法机构的外部支持）。
	分析（RS.AN）：进行分析以确保有效响应和支持恢复活动。
	缓解（RS.MI）：执行活动以防止事件扩展，减轻其影响并解决事件。
	改进（RS.IM）：通过纳入从当前和以前的检测/响应活动中汲取的经验教训，改进组织响应活动。
运营	风险评估（OP.RA）：组织了解组织运营（包括任务，职能，形象或声誉），组织资产和个人的网络安全风险。
	资产管理（OP.AM）：根据组织对组织目标和组织风险策略的相对重要性，确定和管理使组织实现业务目的的数据，人员，设备，系统和设施，以及其中存在的脆弱性和策略
	治理（OP.GV）：管理和监控组织的法规，法律，风险，环境和运营要求的政策，程序和流程得到了解，并告知管理层网络安全风险。
	风险管理战略（OP.RM）：建立组织的优先级，约束，风险容忍度和假设，并用于支持操作风险决策
	供应链风险管理（OP.SC）：建立组织的优先级，约束，风险容忍度和假设，并用于支持与管理供应链风险相关的风险决策。该组织已建立并实施了识别，评估和管理供应链风险的流程。
	应急响应（OP.RS）：执行和维护恢复流程和程序，以确保恢复受网络安全事件影响的系统或资产。
	意识和培训（OP.AT）：为组织的人员和合作伙伴提供网络安全意识教育，并接受培训，以执行与相关政策，程序和协议相关的网络安全相关职责。

- 智安全架构风险控制措施集主要参考了《网络安全等级保护基本要求》、《信息安全管理体系要求》（ISO27001 附录A）的风险控制措施，在此基础上与APDRO五个功能域进行归并、调序、分类。

第二步：风险处置-确定风险控制措施交付物

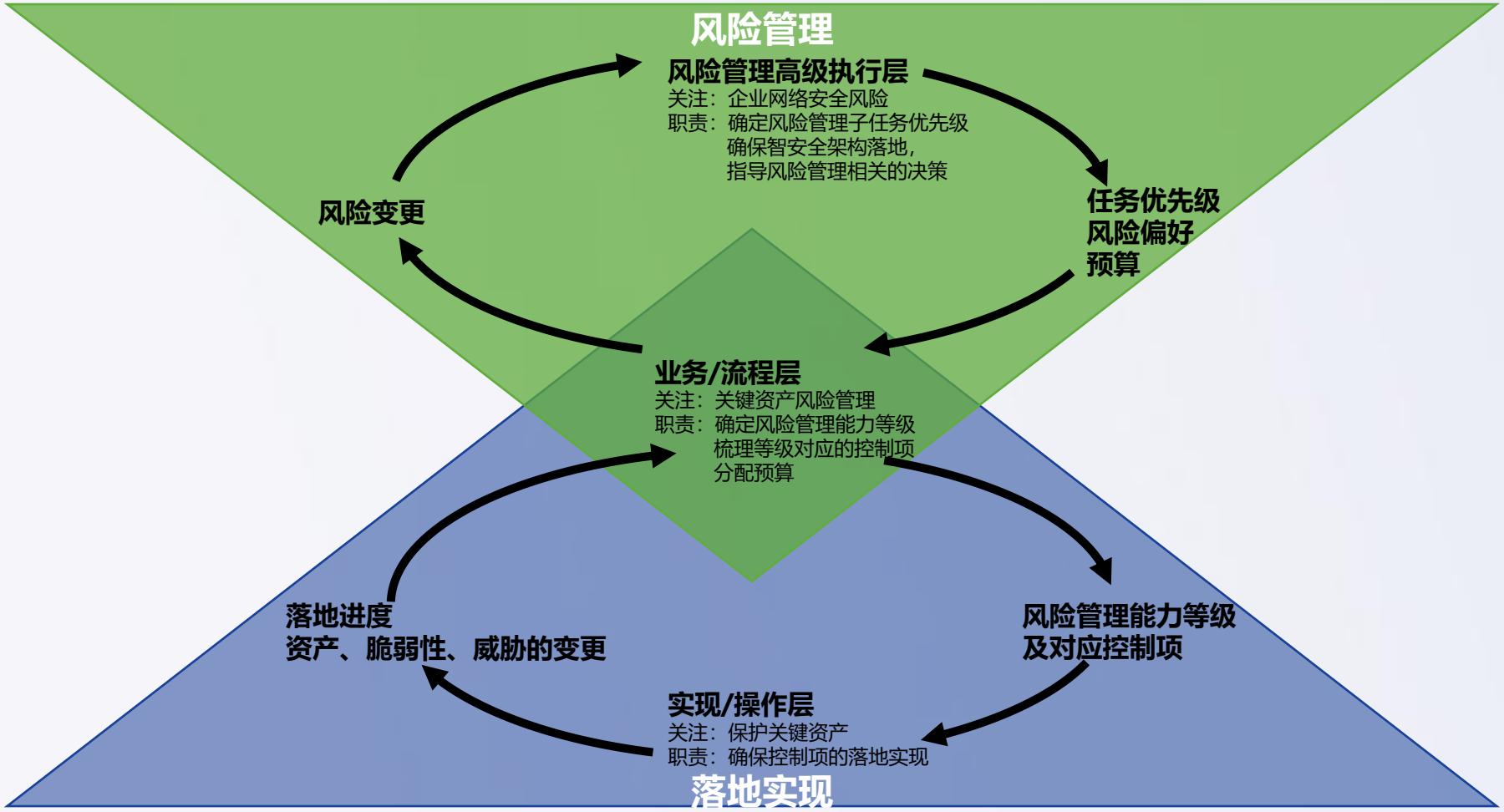


智安全交付模型

场景 \ 安全能力		智能	防御	检测	响应	运营
云	安全资源池					
	云眼&云盾					
	上网安全ISSP					
	云图					
网	下一代防火墙					
	上网行为管理					
	SSL VPN/商密VPN					
	态势感知					
端	企业移动管理					
	终端安全检测与响应					
服务	漏洞管理服务（VM）					
	威胁监测与主动响应服务（MDR）					
	应急响应服务（IR）					

智安全能力交付矩阵

第三步：风险管理体系实现



二、“网端云” 立体保护

网络安全：进一步划分好安全域，缩小攻击面

安全分域	安全域访问原则	
非安全区		
半安全区		
安全区		
核心安全区		
	允许访问	禁止访问

- **非安全区**

  非安全区是数据中心等关键区域与外部直接连接的区域，属于非信任区域，对经过此区域的数据流应进行严格的安全控制；

- **半安全区**

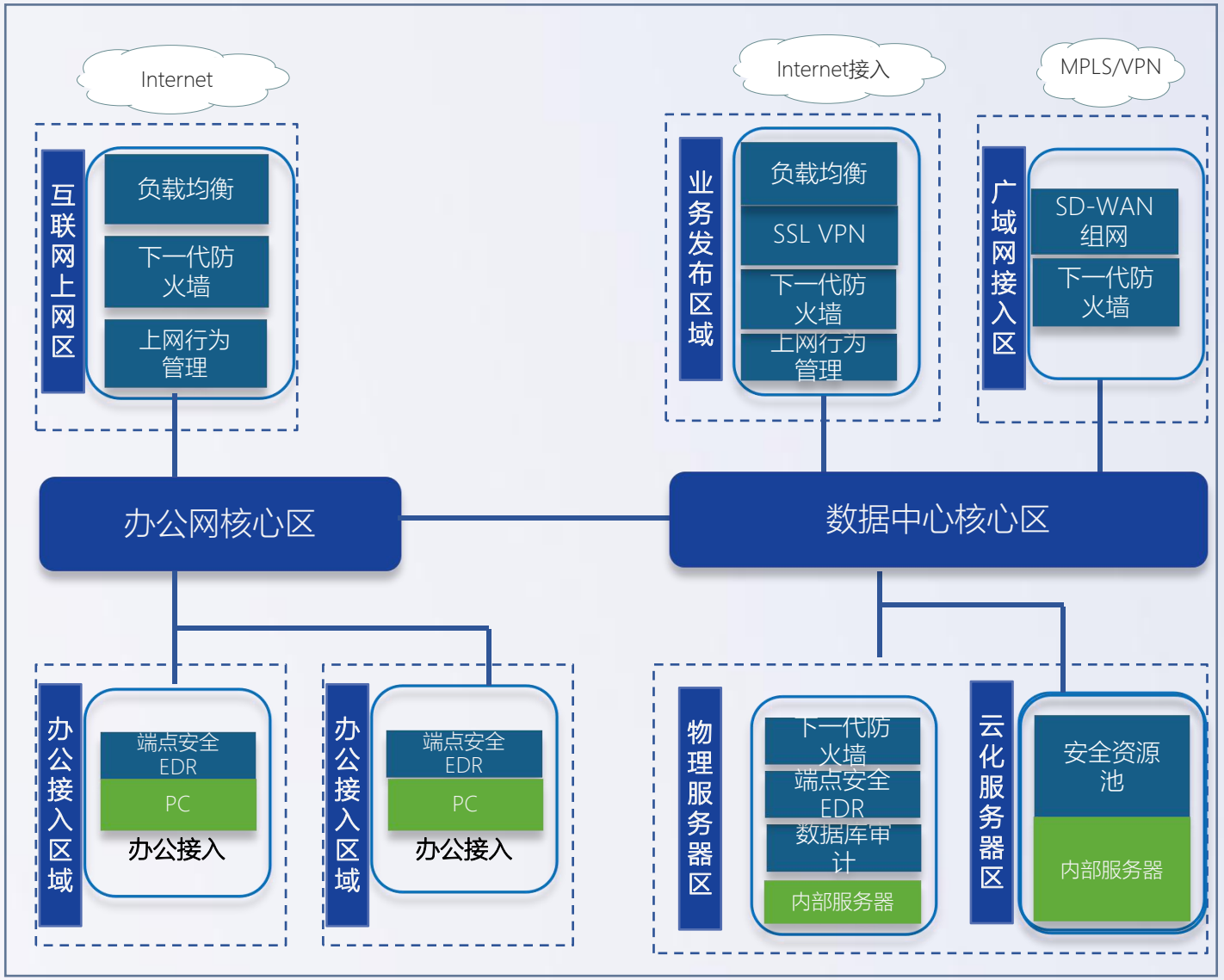
  半安全区是非安全区与安全区之间的过渡区域，用于分割它们之间的直接联系，隐藏安全区的内部资源。此区域通常部署所有与外部连通、为非信任来源提供服务的系统和设备，如VPN、DNS、Proxy、Web、前置系统等服务器。

- **安全区**

  安全级别较高，包括数据中心核心交换、业务测试区、次核心业务区属于安全区；

- **核心安全区**

  安全级别最高，核心业务区都属于核心安全区。核心安全区属于被信任区域；从非安全区、半安全区到核心安全区不允许有直接访问。



网络安全：端到端的边界安全重构

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

•重构终端边界安全

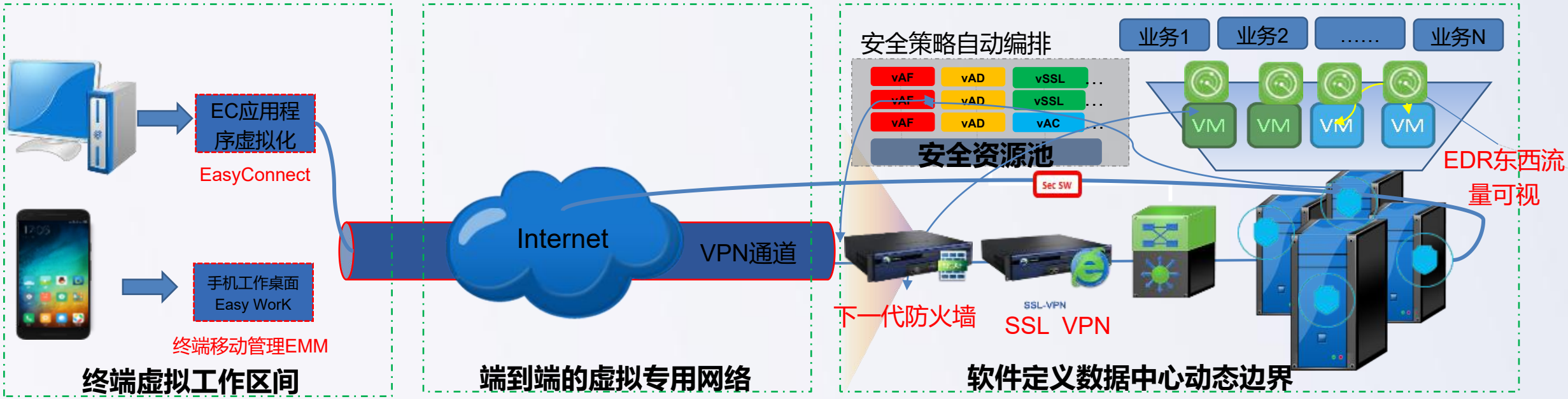
- 把边界退守至终端
  - –移动办公环PC境下，基EasyConnect实现远程应用发布功能
  - –移动手机办公环境下，基于EMM构建独立的工作桌面

•打造端到端传统纵深边界安全

- 端到端的纵深边界安全
  - 多种认证模式，进行内外部身份加固，防止身份冒用
  - 部署下一代防火墙实现数据中心边界防护
  - 基于安全资源池实现数据中心内部的纵深边界防护

•基于软件定义实现动态边界安全

- 基于软件定义，策略自动编排
  - 通过安全资源池的动态编排，可灵活适应业务变化调整
  - 基于EDR软件，可以实现安全策略跟随虚拟机漂移，并实现东西向流量防护



网络安全：纵深边界安全防护最佳实践

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

精细化资产攻击面管理

- **资产可视**
  - 全面识别资产&访问关系，提供业务调整证据
  - 及时发现下线业务并删除策略
- **高危端口可视**
  - 识别违规、不合理的管理端口开放，控制特权服务访问
  - 识别病毒、黑客常利用的端口，减少攻击面
- **策略智能调优**
  - 失效/冗余/冲突等高危策略自动梳理，确保安全策略更有效、更合规

场景化安全防护最佳实践

- **防黑客渗透**
  - 基于黑客攻击链视角，多节点阻断黑客攻击
- **防内网病毒扩散**
  - 针对病毒扩散传播路径（高危漏洞、弱口令账号、共享文件）进行专项防御
- **办公环境安全性&连续性保障**
- **资产失陷外连泄密防护**
- **……**

网络安全：构建统一的安全接入平台

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

端到端的移动安全

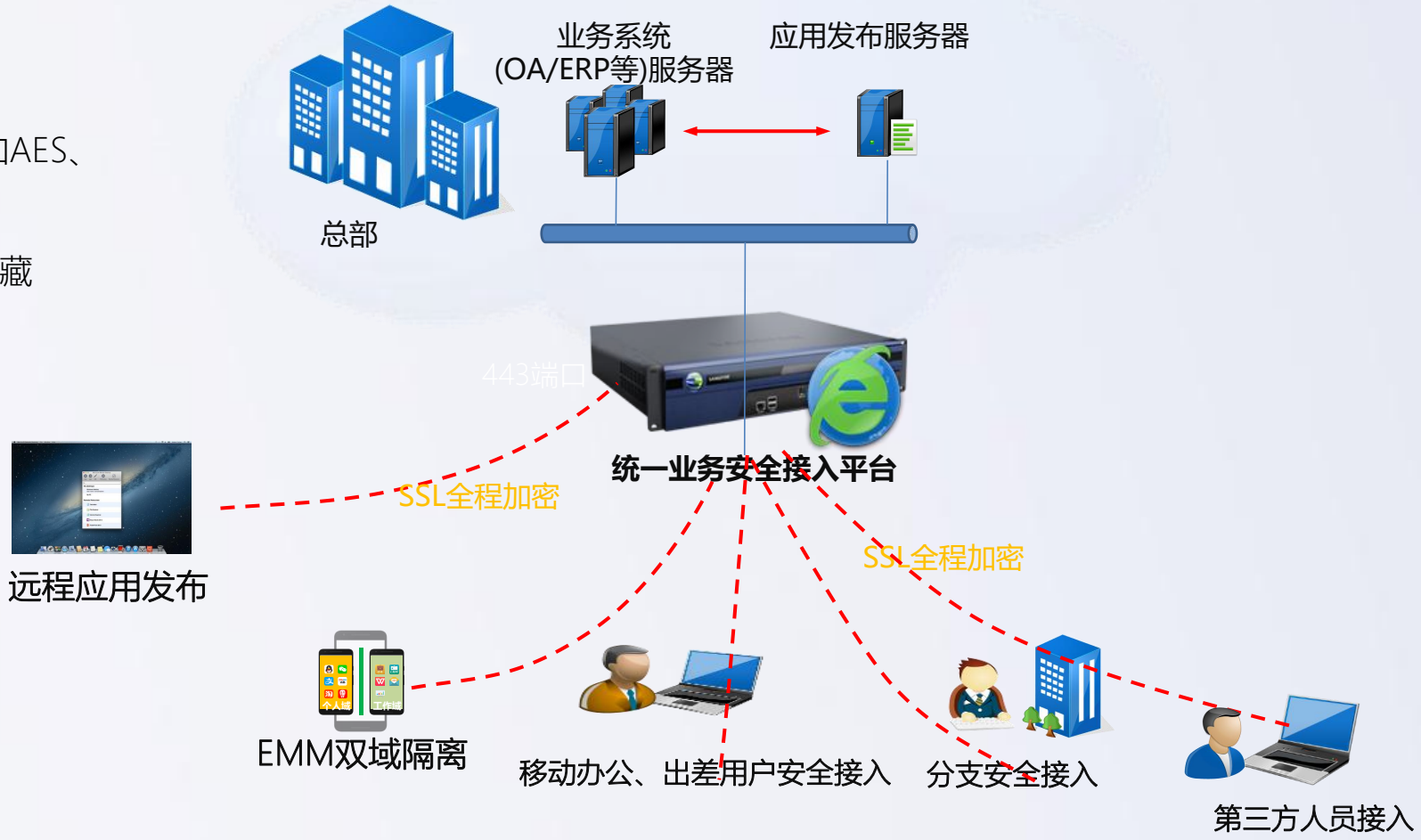
- 多达9种身份认证方式，精准认证无失误
- 角色授权、URL级别授权
- 支持1024位、2028位商密或国密算法，如AES、DES、3DES、RSA、RC4
- 主从账号绑定、服务器地址伪装、应用隐藏

创新的移动终端安全

- 移动终端双域隔离（个人域、工作域）
- 防中间人攻击、客户端安全检查
- SSL专线、客户端零痕迹

用户体验更好

- Htp协议、数据加速、应用加速算法
- 无缝支持多种操作系统平台、终端



打造安全、快速、稳定、易用、易管理的统一移动安全接入平台

网络安全：加强上网行为管控，减少内部风险

上网行为可视

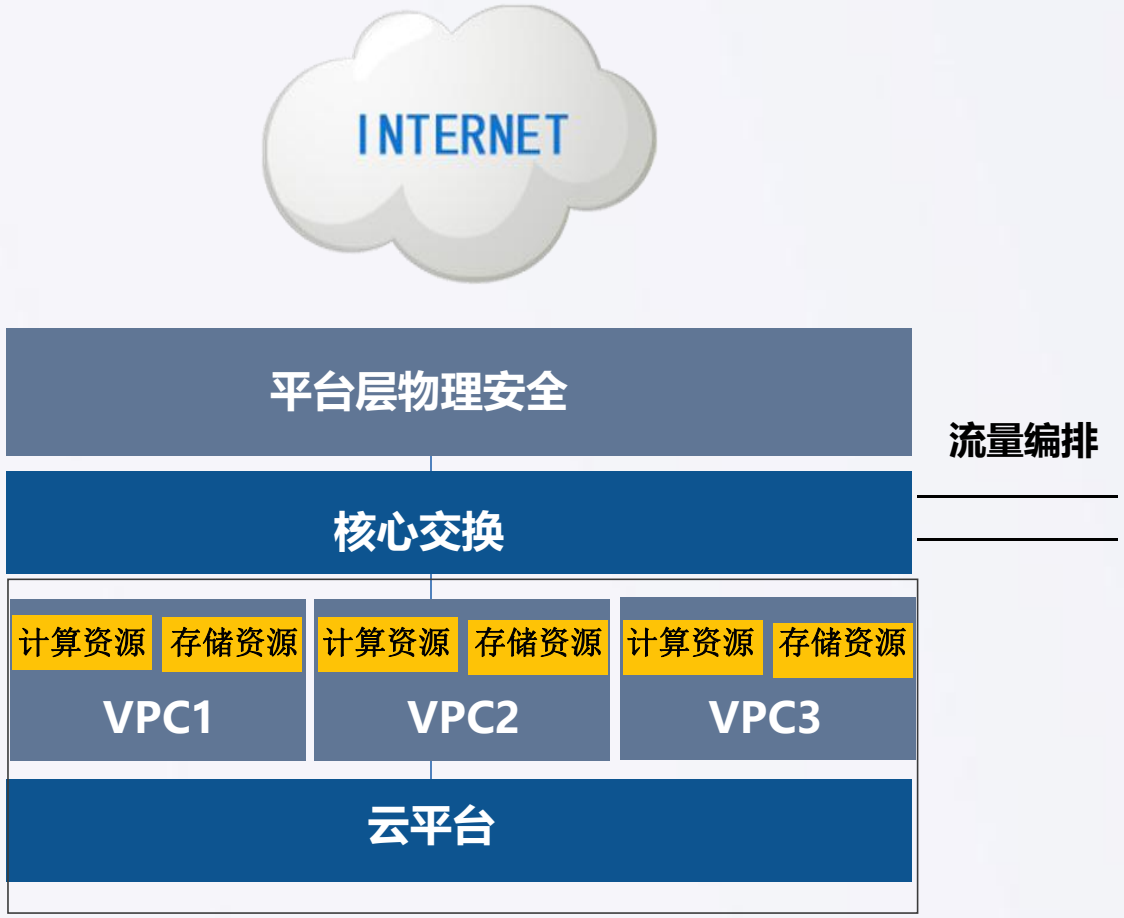
- **用户可视**
  - 有线、无线统一管理（含非法WIFI热点管理）
  - 支持AD域等现有系统整合
- **流量&应用可视**
  - 应用流量准确识别
  - SSL加密流量、P2P流量、移动流量识别
- **内容可视**
  - 应用标签化
  - 深度内容可视，聊天内容、邮件、论坛内容可视

上网行为可控

- **工作效率提升**
  - 通过应用控制，限制与工作无关的上网行为
- **流量可视可控**
  - 合理分配带宽，动态调节，减少浪费，提高带宽应用价值
- **规避法律法规风险**
  - 记录审计用户上网行为，避免肆意外发非法言论

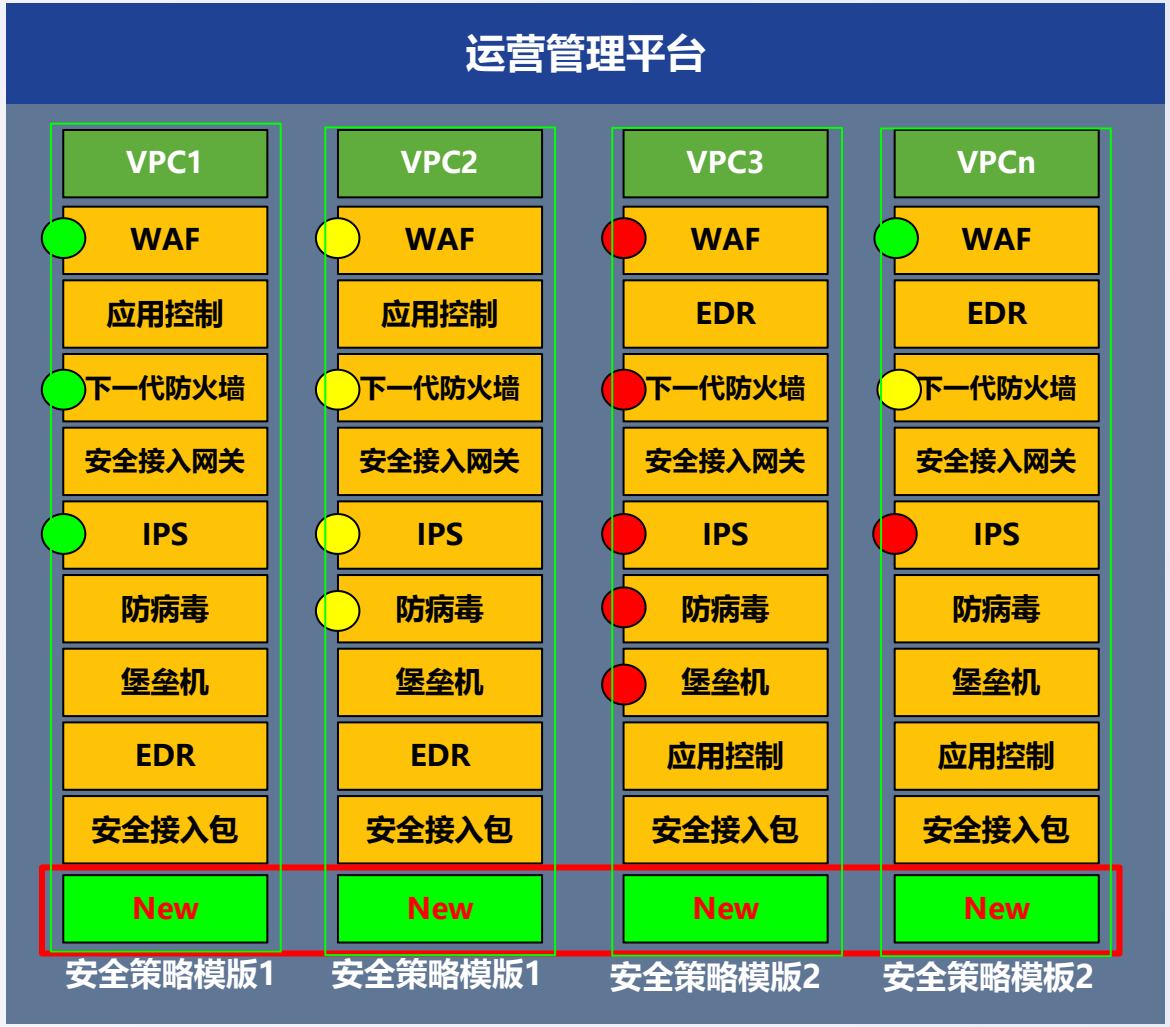
网络安全：软件定义安全资源池，适配云计算环境

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

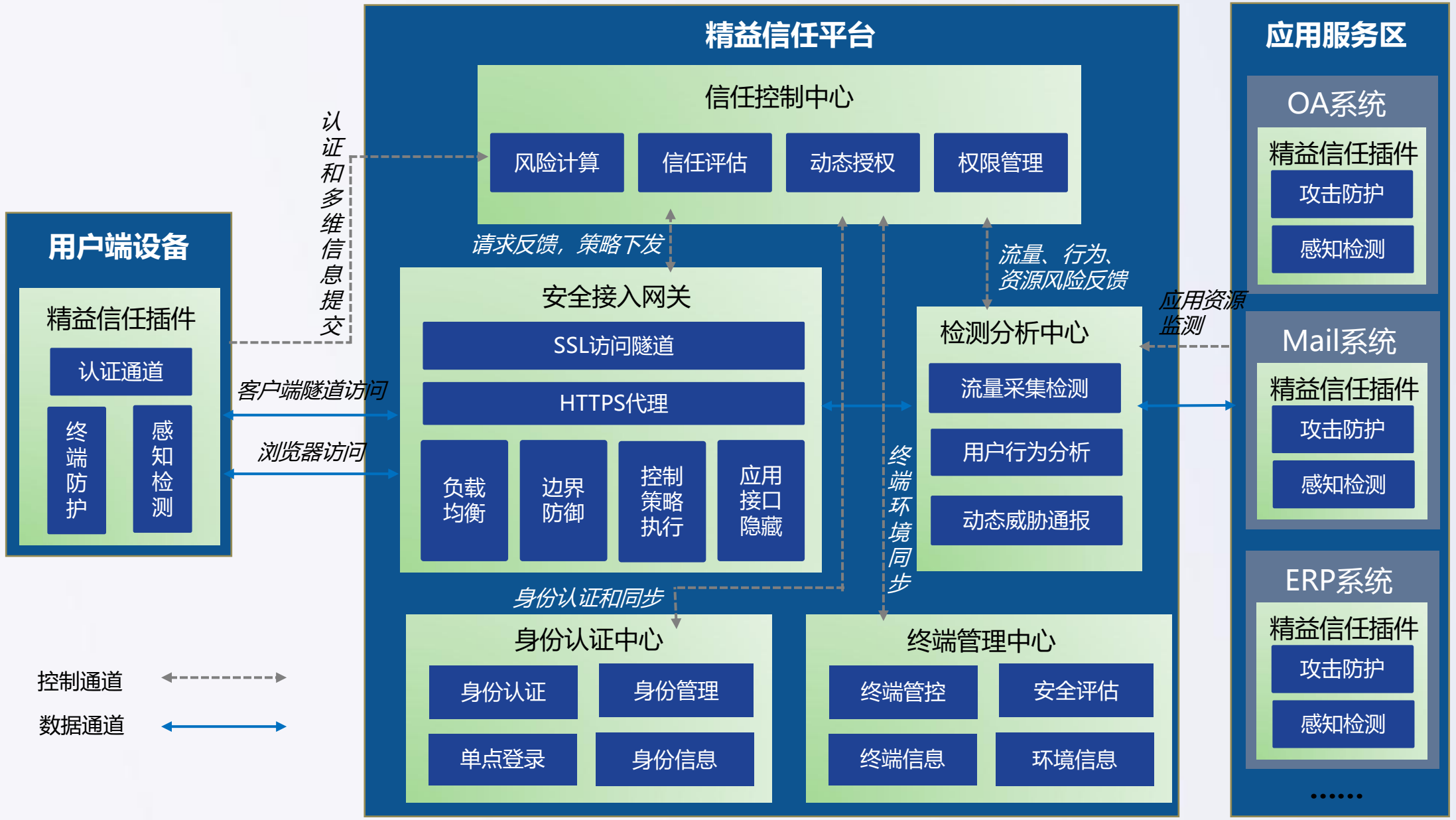


流量编排

云安全资源池：云上的安全AppStore



网络安全：基于精益信任，进一步重构网络边界



网络安全：构建“自动响应、快速闭环”安全大脑

为有效应对未来复杂的快速攻击，我们需要更自动化的响应能力和更高效的闭环能力，这就需要一个集**“集安全风险感知、预测、决策和协同处置为一体”**的**“现代化攻防对抗能力中心”，并拥有“精准、高效、易用”的出色能力，我们把这样的一个中心，称为“安全大脑”**，该理念契合当下“智慧、智能”的时代特点，基于“人工智能和大数据技术”实现安全数据到安全能力的转化。

多源数据输入

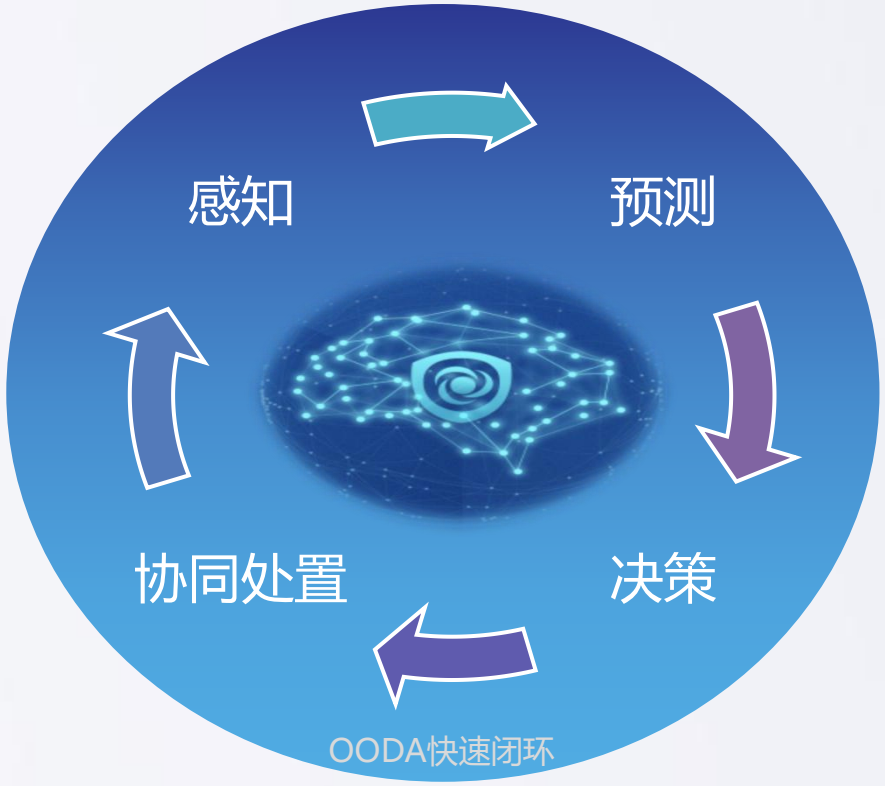
内网安全告警数据

外部威胁情报数据

全流量采集数据

相关业务数据

资产信息



安全能力输出

全面安全态势评估

未来风险预测

快速联动处置

未知、新型威胁对抗

安全绩效输出、辅助决策

数据 → **AI+大数据** → **能力**

网络安全：“安全大脑”整体框架

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

运营管理层

云盾 云守 云脑
AI大数据分析，在线防御、守护..
云眼 云镜 情报
监测、扫描、威胁情报，全面掌控风险..
在线专家
云端运营服务

安全运维服务
在线专家 后台专家
工单触发 工单处置 反馈建议

事件分析、上报

触发人工服务

安全集中管理
设备监控 策略联动 告警推送 订阅服务

安全态势感知
攻击流量分析 病毒木马事件 UEBA行为分析 事件追溯

设备的集中管控、联动控制

采集资产、威胁数据

运营保障机制
运营组织
运维流程
日常运维机制
应急响应机制
规章制度

安全设备层

安全组网：
ABSO一体机
MIG
WOC

边界网关：
下一代防火墙
工业防火墙
上网行为管理
无线IPS

流量探针检测：
采集流量、感知资产、漏洞变化

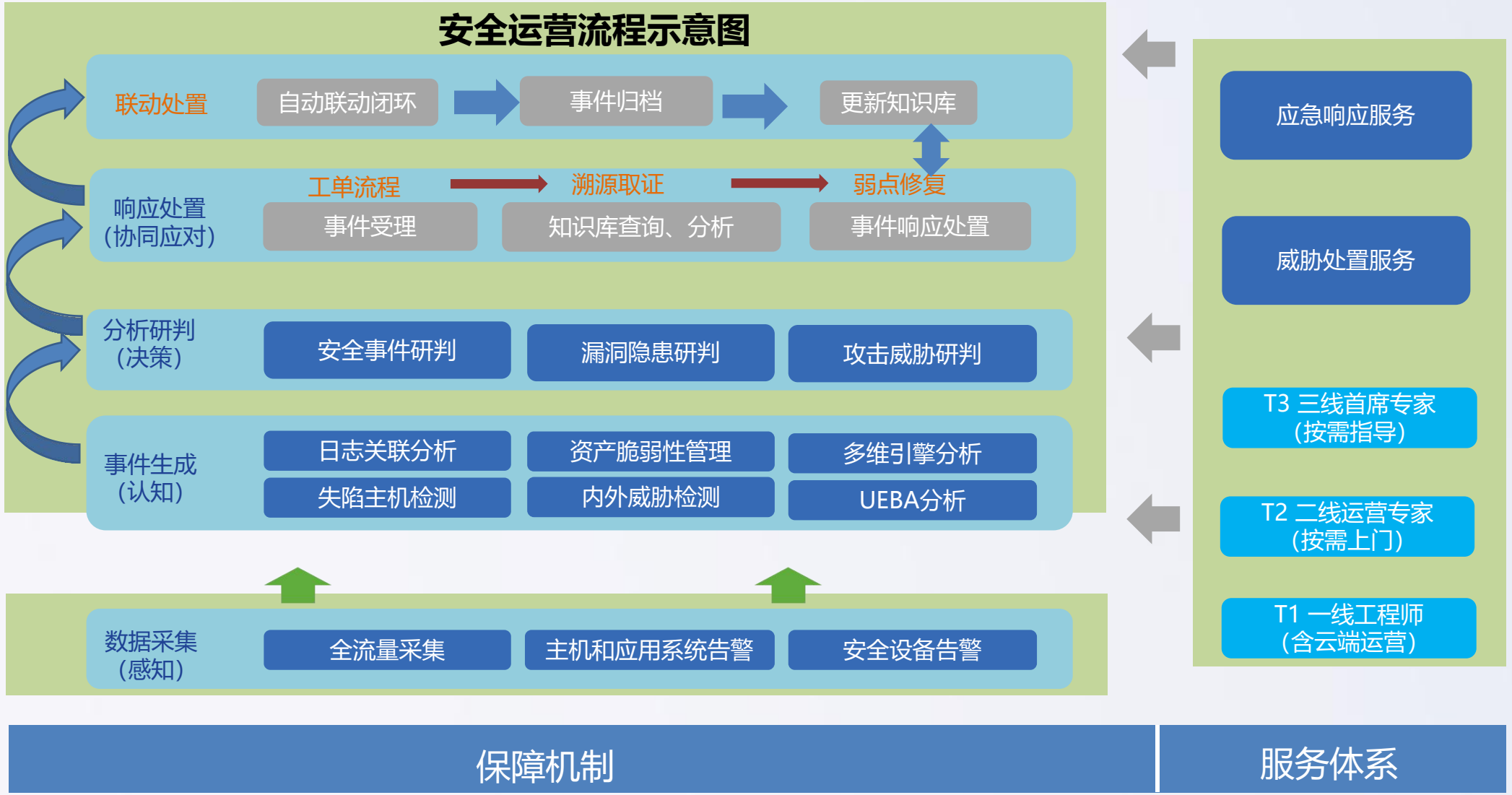
日志采集器
采集交换机、防火墙等日志

主机和工控安全：终端检测响应
EDR、工控安全卫士

软件定义安全资源池：（数据库审计、堡垒机、漏洞扫描等）

硬件边界网关
采集传感器
软件定义安全组件

网络安全：“安全大脑”业务流程



保障机制

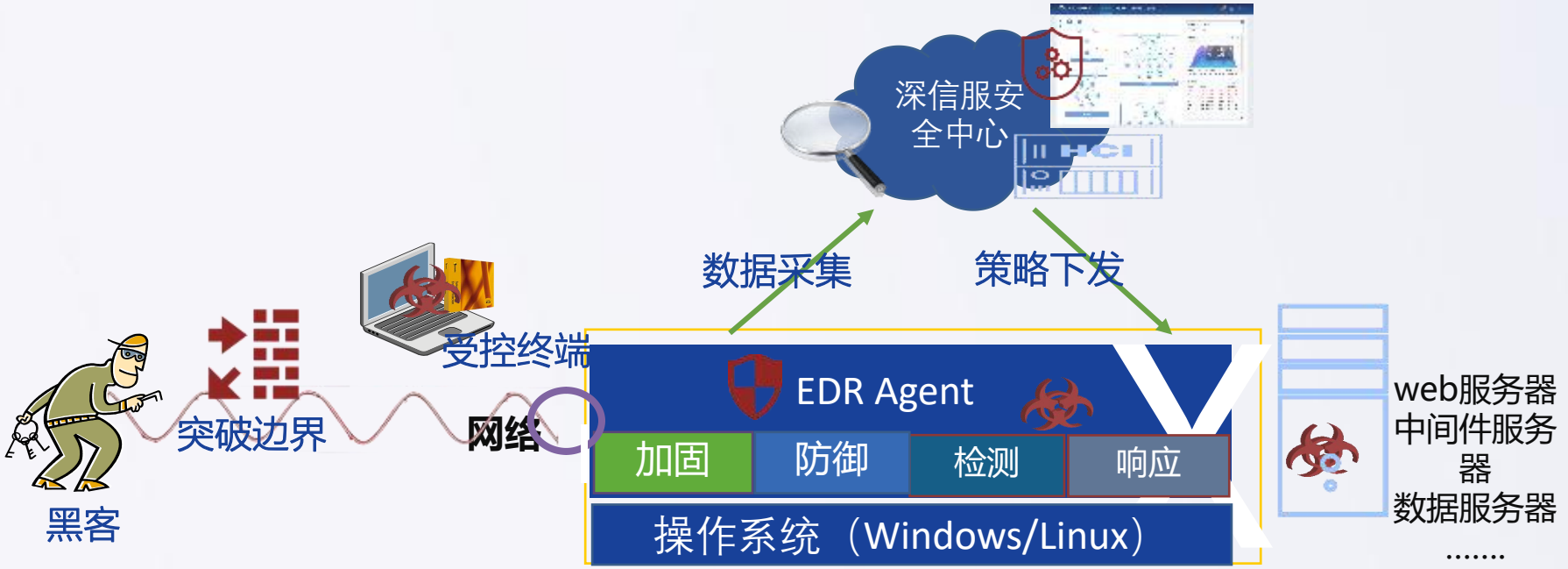
服务体系

网络安全：“安全大脑”全局可视化能力

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

端点安全：加强端点安全建设，筑牢最后一道防线



❶ 加固（微隔离）

基于应用策略，实现主机东西向流量访问控制

- 业务安全域之间
- 业务安全域内部

❷ 防御

全面探测服务器主机和网络上的威胁活动

- 入侵行为主动IP封堵
- 恶意文件隔离

❸ 检测

传统技术+人工智能+机器学习的智能检测模型

- 病毒、木马检测
- 僵尸网络检测
- 暴力破解检测

❹ 响应

监控进程的可疑行为，以即时拦阻恶意代码

- IP黑白名单机制
- 文件隔离机制

深信服方案优势

- **支持多个操作系统**

支持部署在Windows、Linux、Ubuntu等操作系统

- **实现跨平台**

可在PC终端、云平台、物理服务器等各环境部署，与平台无关

- **集中管控**

不论部署的环境和所处地域，均可在统一的Web控制台查看和操作，实现了跨云的统一管理

- **轻量级**

Agent占用不超过1%CPU，内存占用少

端点安全：下一代WAF引擎，提升Web安全能力

多种格式 的恶意代码
(PHP/JSP/ASP ...)

日新月异 各种漏洞
(难以用程序描述)

多种场合 的注入攻击
(SQL / STRUCT2 ...)

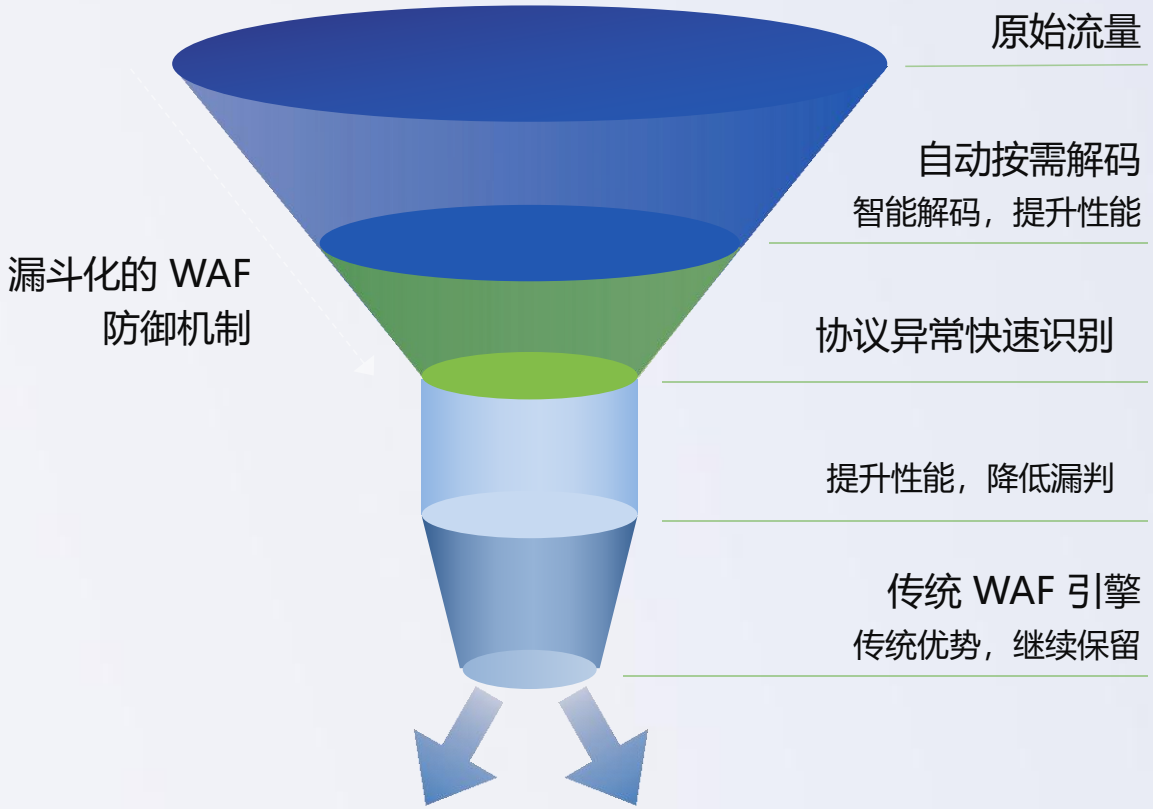
各种难题

.....

传统规则引擎 VS **下一代 WAF 防御**

- ◆ 误判率高
- ◆ 维护困难

- ✓ 更强规则
- ✓ 更少误判
- ✓ 更快响应



（下一代 WAF 防御框架）

端点安全：数据生命周期安全防护能力

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

数据安全组织

数据系统安全管理要求的安全管理组织架构

数据安全目标、策略

分层制定数据安全目标和策略

数据全生命周期安全管理规范

数据产生/采集	数据传输	数据存储	数据使用	数据共享/销毁
数据采集管理	传输和账号管理	数据存储管理	数据使用管理	共享销毁管理
数据类型分类	传输加密策略	存储加密策略	授权管理	数据接受方审核
数据安全责任划分	账号审批流程	数据类型管理	基于业务的控制	数据共享规定
数据安全等级划分	账号状况定期复核	数据保留管理	基于角色的控制	销毁策略
	高危/外包账号管理	数据分层存储	审计策略	恢复测试

对数据全生命周期安全，制定流程化标准化灌流规范

业务连续性管理

制定管理规范，保障数据系统具有应对风险、自动调整和快速恢复能力

安全合规管理

及时发现规章、制度、规范执行情况，根据合规检查结果进行优化调整

专业安全服务

三级服务响应机制，快速响应，数据安全设计支持与咨询、安全方案与系统测评

端点安全：信息防泄漏，保护敏感数据

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

数据行为可视：

- 数据防护海量日志分析

图计算、机器学习深度挖掘分析泄密行为，可视化展示统计；

- 泄密风险预警，准确追溯

泄密通道预警，高危行为阻断，以数据为中心的行为追溯

终端泄密防护（桌面云）：

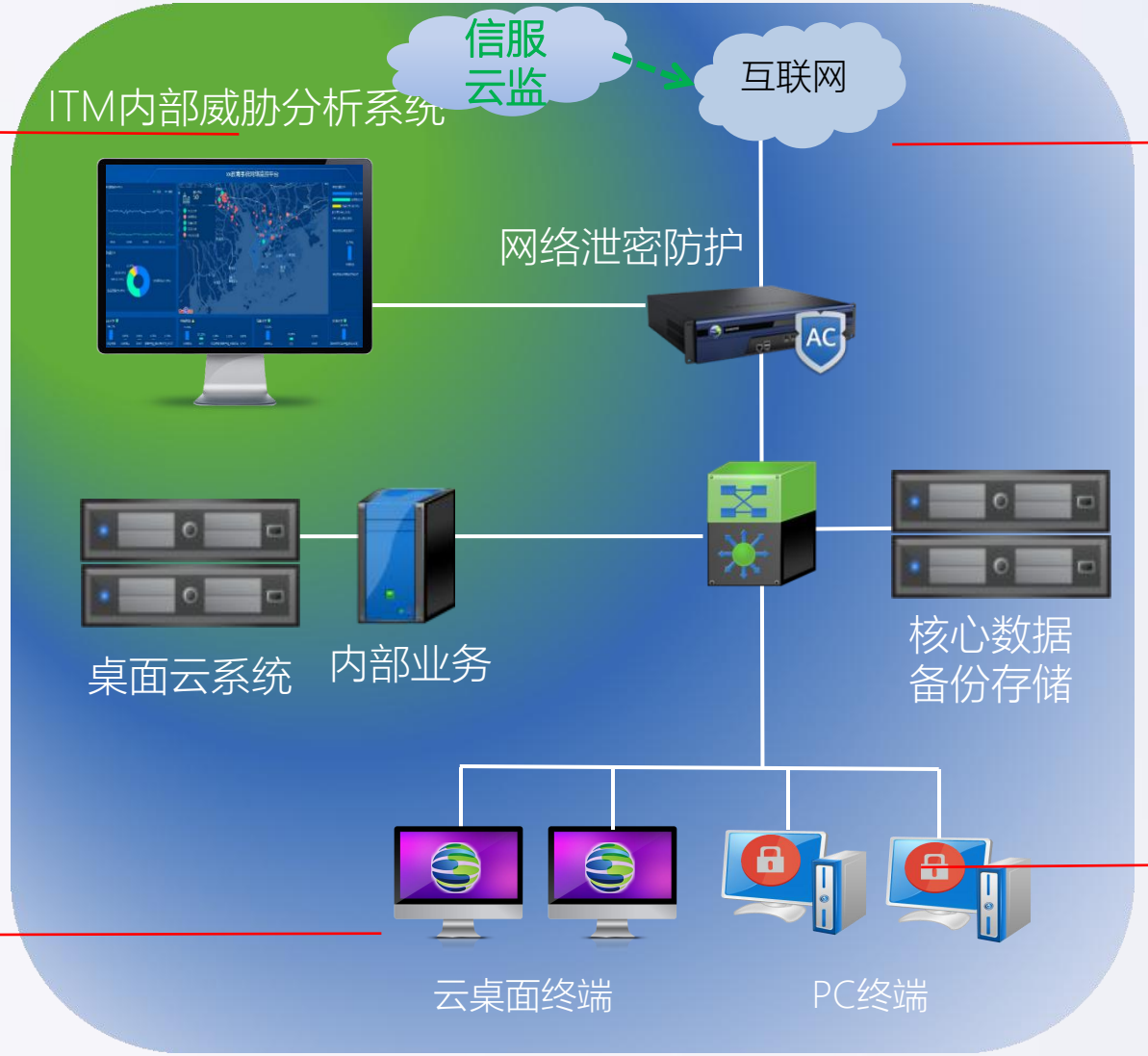
- 数据不落地，杜绝本地数据外泄

云桌面终端，终端0数据，杜绝本地拷贝问题；

精细化的外设策略、应用管控、水印；

- 核心数据定时备份

核心数据定时备份，防止误操作及勒索病毒造成的数据损坏；



网络泄密防护：

- 网络行为控制

识别邮件、网盘等应用流量，封堵外发泄密行为

- 流量内容审计

审计外发文件内容，记录流量行为，事后可追溯

终端泄密防护（PC）：

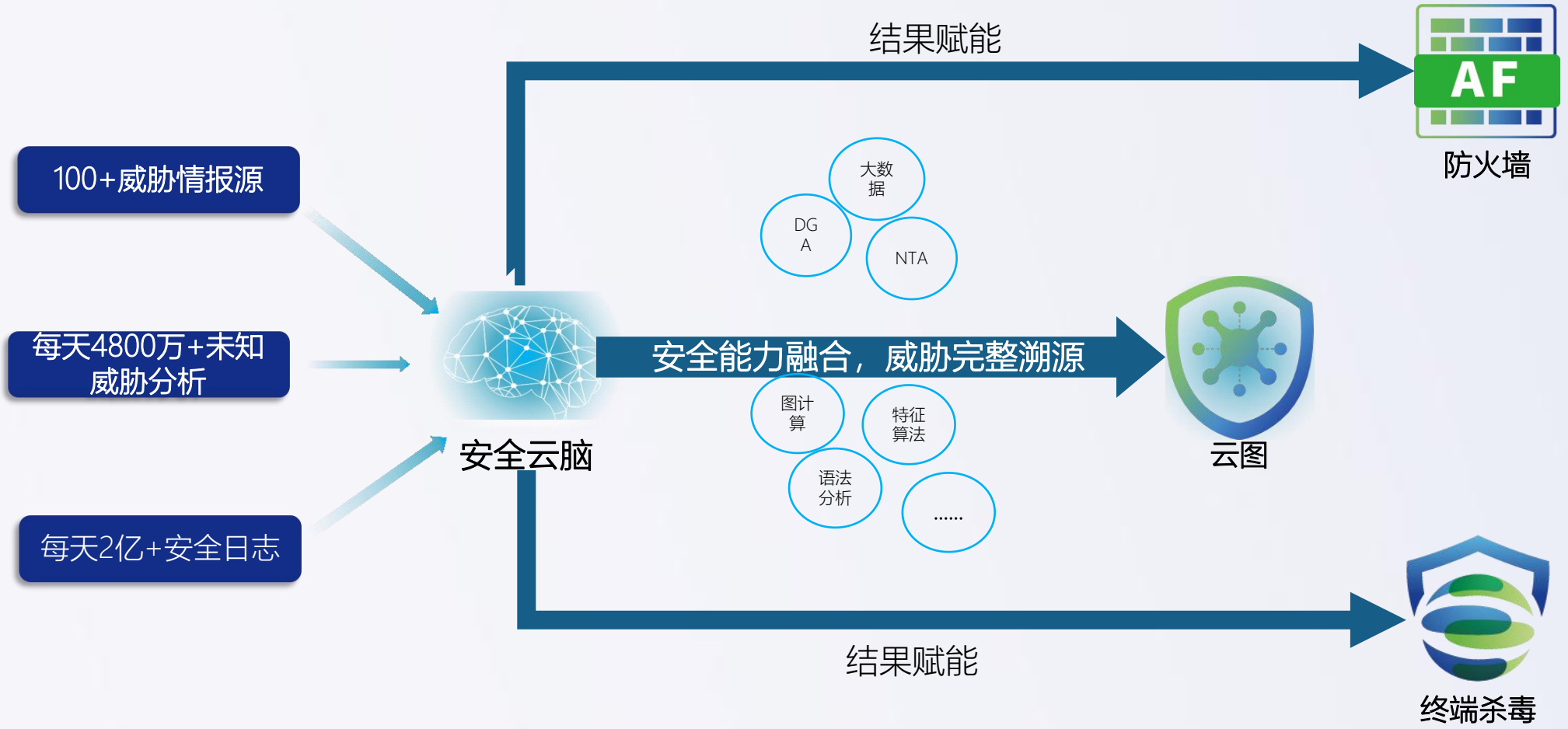
- 文件透明加密
- 文件外发管控、审计
- 外设权限管控、应用管控

云端安全：整体框架

- **安全云脑**：安全云脑作为深信服的云端安全能力中心，通过海量数据汇聚，大数据智能分析与挖掘，鉴定引擎主动进化，设备实时联动，持续在向各产品赋予安全能力。
- **云图及其他**：作为云端安全管理平台，可以让用户通过云端管理所有深信服安全产品，并可将所有安全产品日志统一汇集、分析和呈现，提供云网端联动能力，为用户提供自助安全处置平台，降低用户安全运营复杂度。

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……

云端安全：通过安全云脑持续赋能



云端安全：7X24小时自动化运营

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

可视化的处置中心

多产品安全事件融合展示，云、网、端产品联动处置

实时化的威胁告警

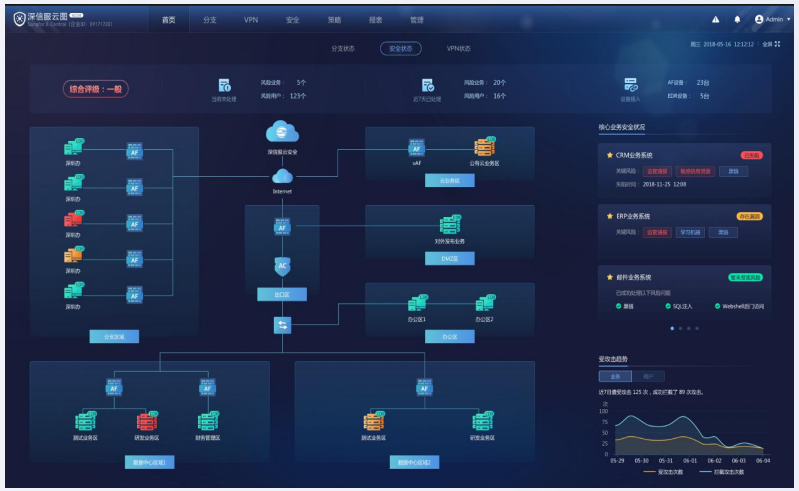
微信实时告警威胁信息，有效压缩威胁扩散窗口期

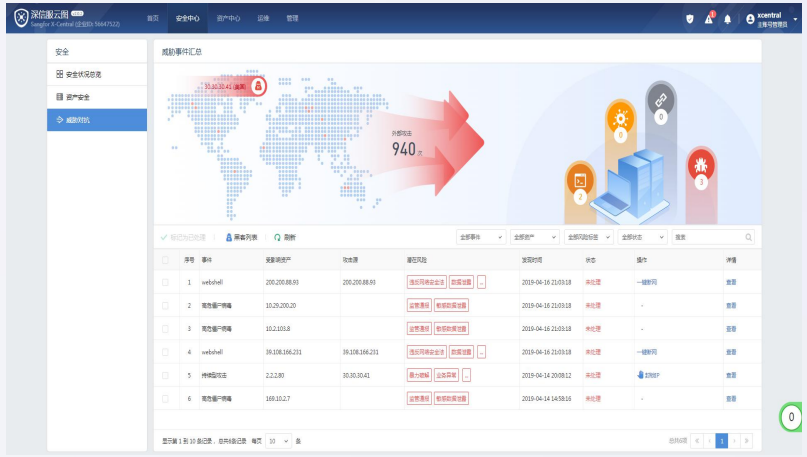
智能化的威胁对抗

基于人机共智的安全理念，利用云端大数据分析能力、安全专家值守分析，有效识别高级黑客、潜在威胁行为，提供从入侵到失陷的安全溯源分析及处置建议

一体化的运维管理

设备监控，统一升级，远程免密登录，云端策略模板编辑、策略统一下发，智能告警，报表分析





三、基于威胁情报的主动防御

威胁情报定义

- Gartner：威胁情报是基于证据的知识，包括上下文、机制、指标、可能的结果和可操作的建议，涉及资产面临的现有或新出现的威胁或危害，可为主体威胁或危害的响应决策提供依据。

总体流程

数据 → 智能 → 能力

数据采集

- 网络数据
- NGAF
- AC
- 安全感知系统
- 云眼、云盾、云镜
- CNCERT
- Virus Total
- ……

数据管理

- 数据清洗
- 数据脱敏
- 存储管理
- 预处理
- 威胁情报
- ……

安全云脑

人机共智：

- 攻防专家
- 数据科学家
- 安全分析师

弹性智能：

- 规则
- 特征
- 无监督学习
- 半监督学习
- 有监督学习
- 时间序列分析
- ……

能力构建

- DNS Flow
- Http Flow
- Webshell
- 扫描
- 僵尸网络
- 恶意URL
- 黑链检测
- ……

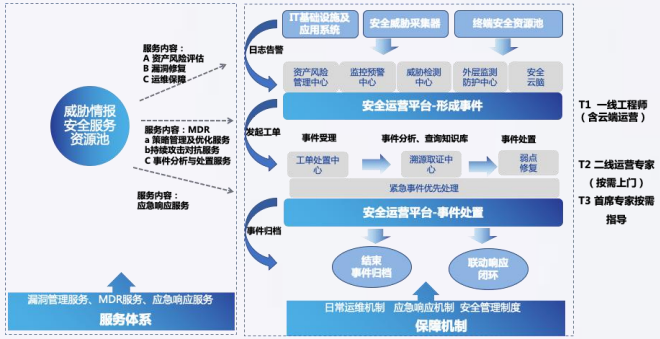
升级 ← 能力

情报驱动的主动防御体系

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

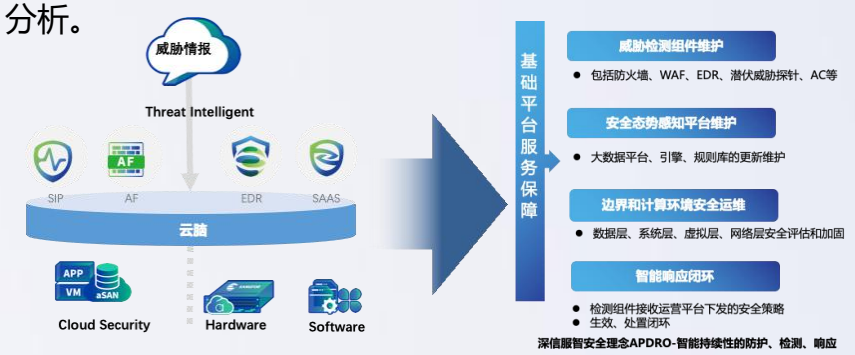
情报驱动应急响应体系

深信服威胁情报中心实时跟踪热点漏洞事件，帮助安全运维人员尽快完成确认、分析、修复工作，并确认修复效果。



利用情报聚焦关键风险体系

利用外部威胁情报，快速定位影响本地资产安全的关键风险点，结合业务系统资产重要等级，给出更为有效的风险评估分析。

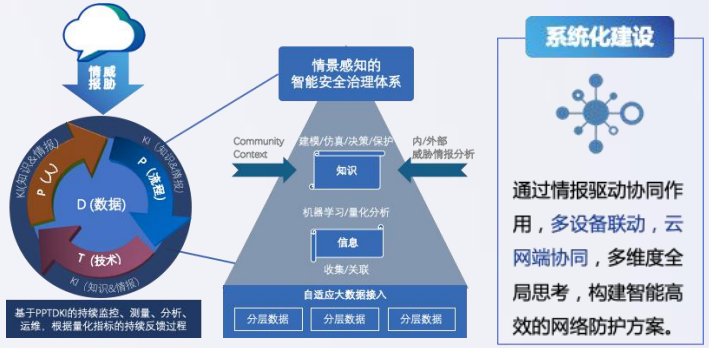


情报驱动资产持续监控体系

对采集到的情报、脆弱性数据进行预处理，排除重复、无用数据、尽量消除误报信息，是最终评估分析结果更为精确。

情报驱动安全治理体系

基于情报赋能PPTDKI的持续监控、测量、分析、运维，根据量化指标的持续反馈过程。



总结：深信服安全建设规划思路

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

企业安全建设规划思路

- 风险驱动
- 立体保护
- 主动防御

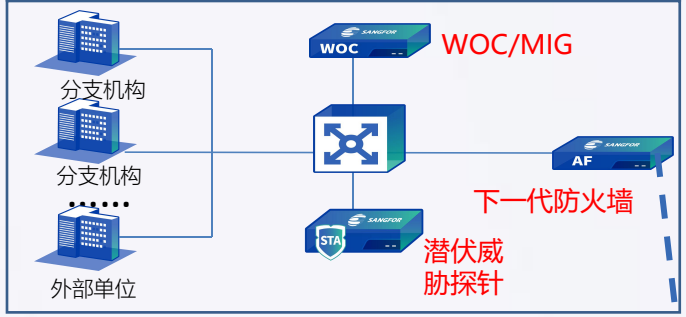
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

参考网络拓扑

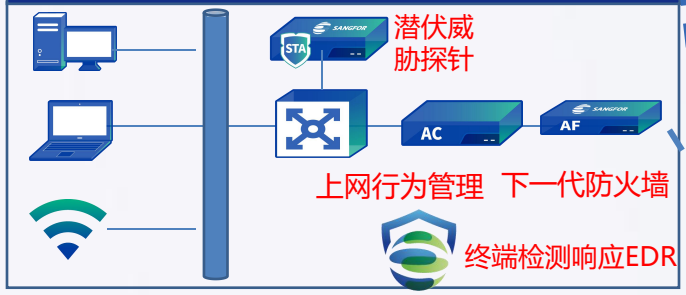
网络安全拓扑参考

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

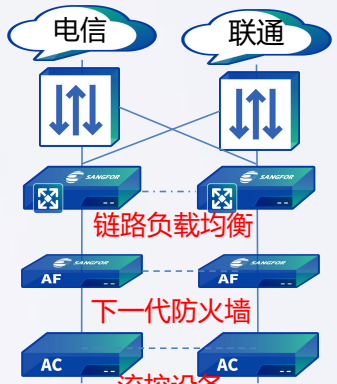
安全接入区



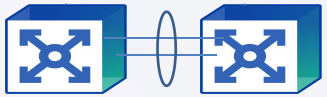
办公终端接入区



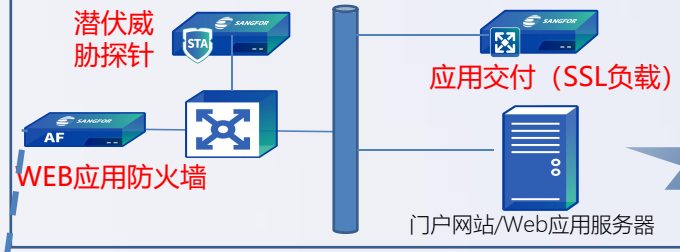
互联网出口区



核心交换区



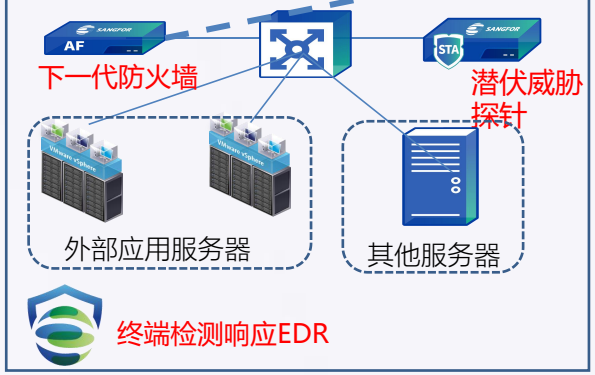
DMZ区



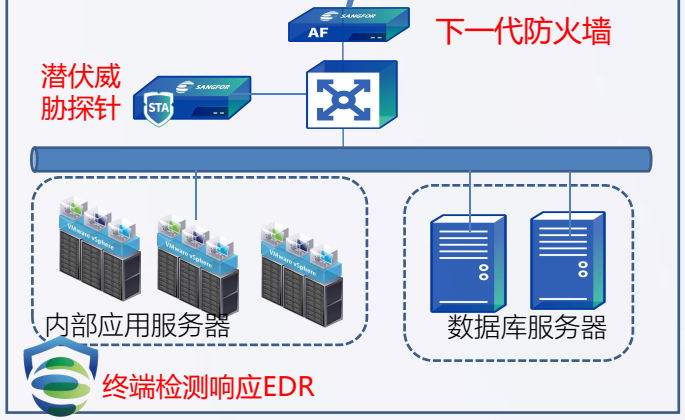
安全管理区

云端安全

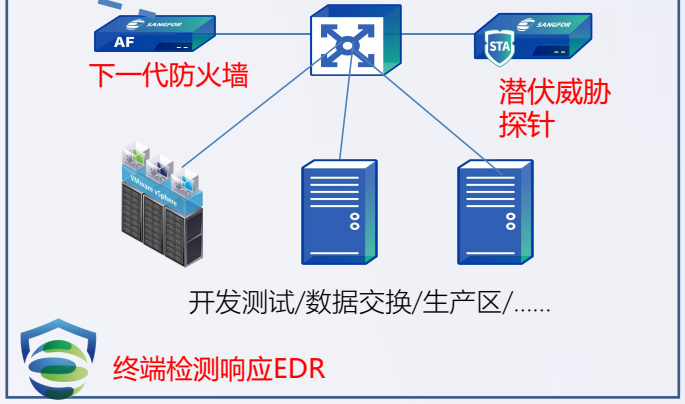
外部业务区



内部业务系统区



其他区域



配套安全服务

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

一．信息安全现状与挑战

二．深信服的理解与建议

三．我们提供的解决方案

四．技术能力与客户案例

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

技术能力

全面领先的安全厂商能力

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

领先的产品技术

多款安全产品市场占有率第一

- 硬件VPN产品市场份额第一
- 上网行为管理产品市场份额第一
- SSL VPN产品市场份额第一
- 广域网优化产品市场份额第一
- 下一代防火墙在综合类防火墙品类场份额第二

国际认可

- ICSA防火墙认证
- OWASP测评四星
- 中国唯一获NSS Labs“Web攻击防护”最高评价“推荐”
- AC、WOC、SSL VPN是唯一入围国际Gartne魔力象限的国产品牌

广泛的生态合作

战略合作伙伴

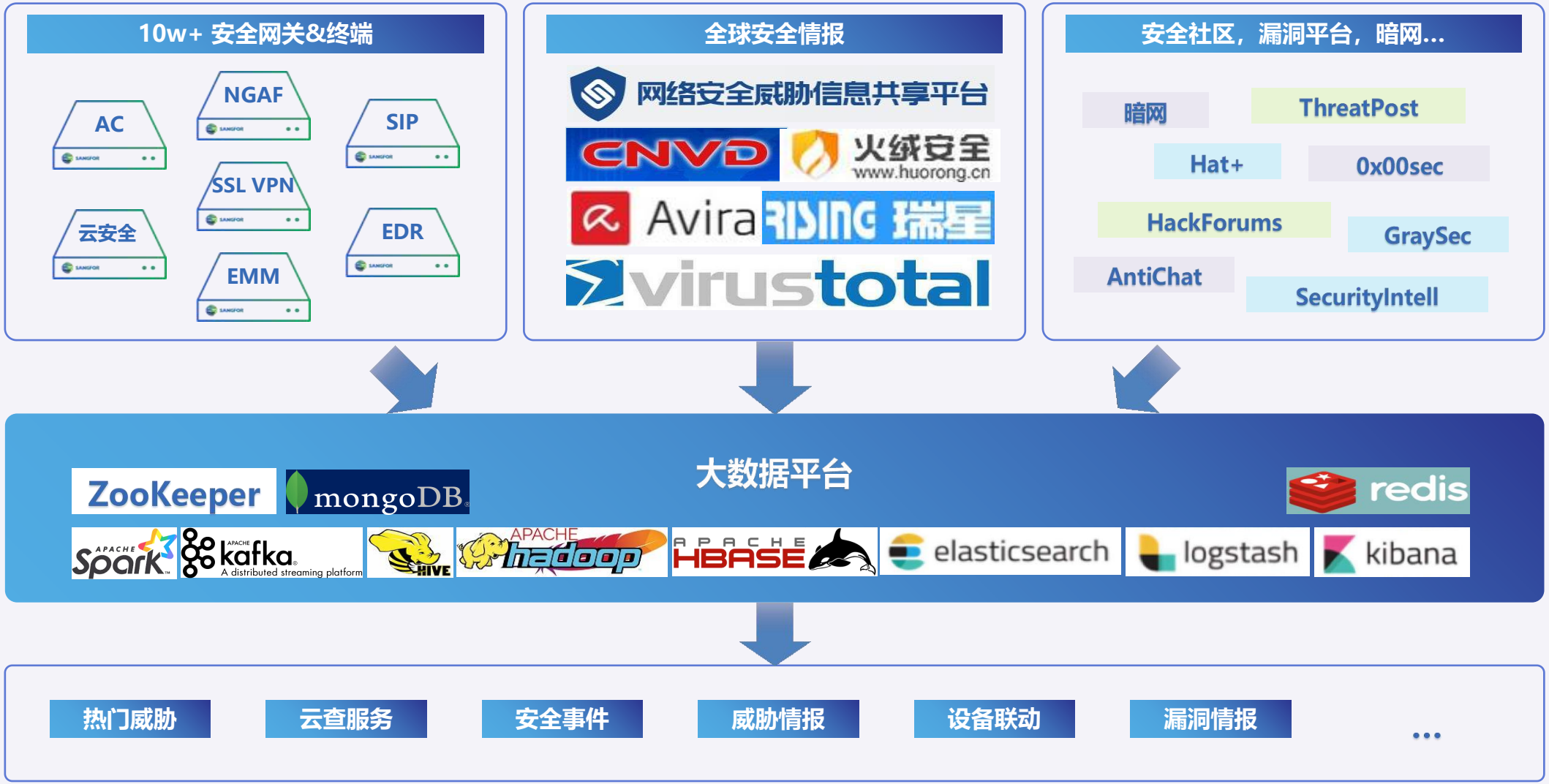
Microsoft | intel | redhat | NVIDIA | 腾讯云
阿里云 | aws | Baidu 百度 | HUAWEI | inspur 浪潮

安全解决方案合作伙伴

吉大正元 | Avira | KASPERSKY | RISING 瑞星 | 火绒安全 www.huorong.cn
JIANGMIN 江民科技 | 圣博润 SBR-info | 思福迪 SAFETY | 建恒信安 JIAN HENG XIN AN | 云安宝
WebRAY 盛邦安全 | JUMING 聚铭 | 安盟信息 SECURITYUNION | victory idea 信恩信安 | 联软科技 LEAGSOFT
Infogo 盈高科技 | Softnext 守内安信息科技 | ANTIY 安天 | 兰云科技 LANYUN TECHNOLOGIES | 兰德网络 LANDE NETWORK | 摩卡 Mocha
6cloud 六方云 | THNWIN | Oplead

海量企业级安全数据积累

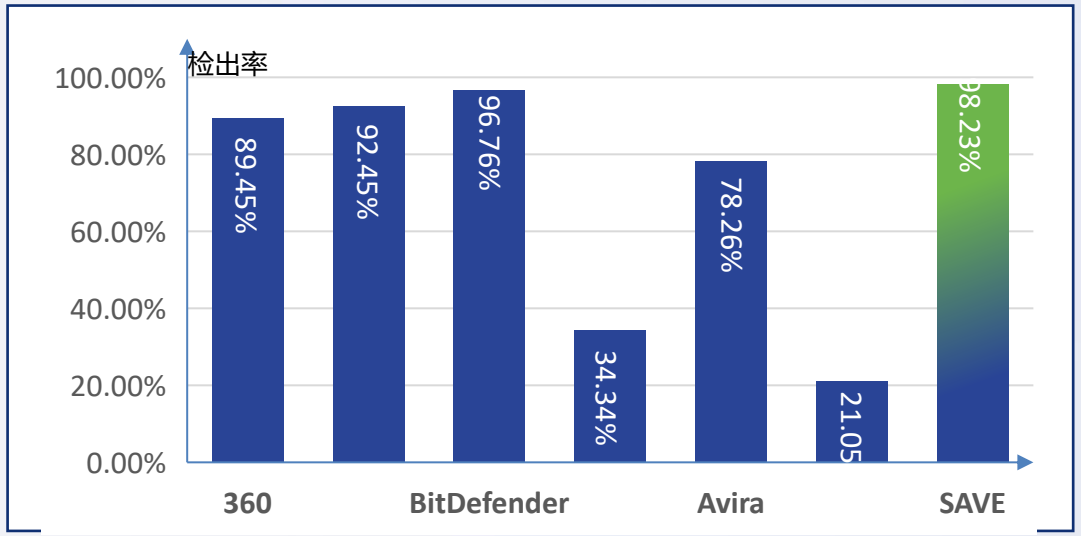
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY



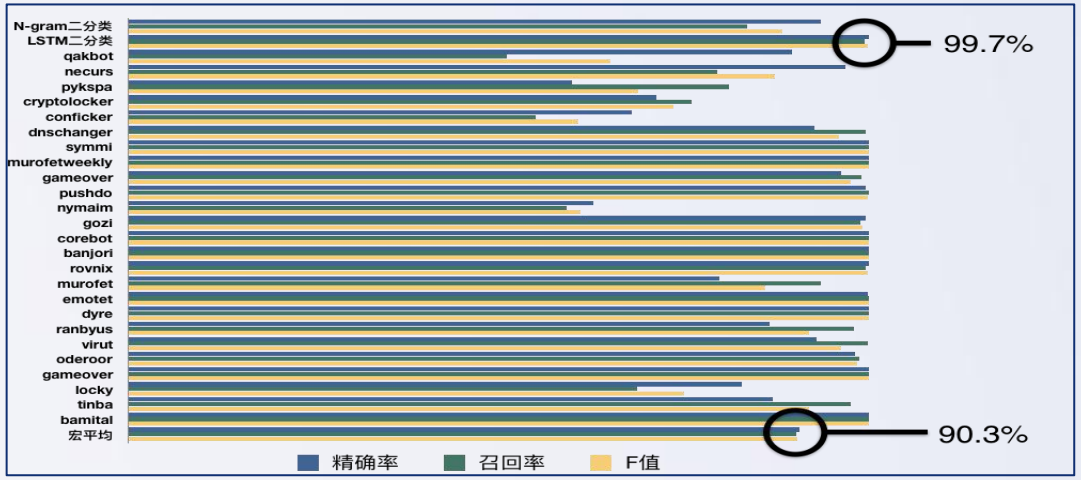
全面精准的高级威胁检测能力

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

- 流量行为分析建模
- 文件威胁智能鉴定
- 异常行为分析
- UEBA用户行为基线
- 失陷主机检测



千万级样本的测试， 人工智能SAVE处于业界领先的水平



基于机器学习行为分析的僵尸网络检测检出率达到99.7%

僵尸网络：行为特征->机器学习->神经网络

硬编码域名检测

域名独报率超过70%

➢及时发现随机性强、变化快的僵尸网络域名
➢采用行为检测，不是单纯的黑名单匹配，对客户具有更强的可解释性

"v1.tbkpridy.com",
"v1.qtlmzqwq.com",
"v1.sxpmacqp.com",
"v1.nlrkwrsc.net",
"v1.jsjlulwi.com",

主机访问超过30条此类域名

单一域名规则均不属于很强的情报，VT上只有两个厂商检出，但主机访问大量这样的域名则足以说明主机的失陷

DGA检测

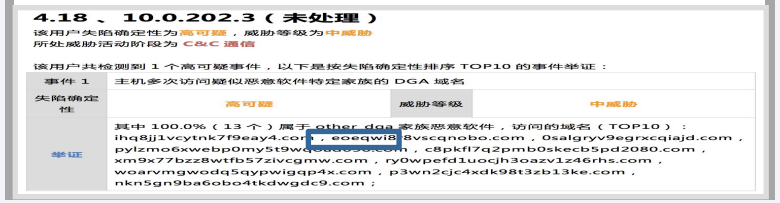
高检出、低误报、强泛化

➢ 蓝军测试团队对DGA2.0文法特征模块测试

检出率（检出DGA域名数/测试DGA域名数）	误报率（白域名报为DGA数/测试白域名数）
97.50%	2.70%

➢ 配合行为检测，基本无误报

➢ 在某省建筑设计院发现的未知恶意通信，后确认为新型恶意软件“狮鹫”



湖北某大学Beta点与知名友商对比测试，取得明显优势。
检测时间2018/10/28~2018/11/01

	DGA检出事件数	误报率
深信服	436	0.00%
友商	340	37%

LSTM算法

僵尸网络检出率达到99.7%，并能追溯病毒家族(业内领先)

长短期记忆神经网络LSTM

人工智能SAVE引擎，业绩领先

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

千万级样本的测试， SAVE业界领先

多例变种首发

近日，深信服安全团队追踪到**公有云上及外部Linux服务器存在大量被入侵，表现为/tmp临时目录存在watchdogs文件，出现了crontab任务异常、网络异常、系统文件被删除、CPU异常卡顿等情况，严重影响用户业务。**多个用户邀请深信服安全专家远程排查，最终经过分析确认，用户Linux服务器被植入新型恶意挖矿蠕虫，且较难清理。

深信服安全团队将其命名为WatchDogsMiner，并紧急发布预警，提醒企业用户及时开展自查修复，防范WatchDogsMiner挖矿蠕虫。

近日，深信服安全团队在国内跟踪发现了一新型的勒索病毒变种，确认为GandCrab家族的最新版本GandCrab5.1。国内感染案例以RDP爆破为主，通过人工入侵和手工投毒，专门攻击数据库服务器。

针对GandCrab5.1新型勒索变种，深信服SAVE安全智能检测引擎，通过对已知病毒的深度学习，无需更新规则，即可直接快速检出！

第三方知名测评机构认可

赛可达实验室

4 测试结果总结

测试项目	测试结果
恶意软件检测	98.51% - 通过
误报率	0% - 通过

赛可达实验室

5 结论

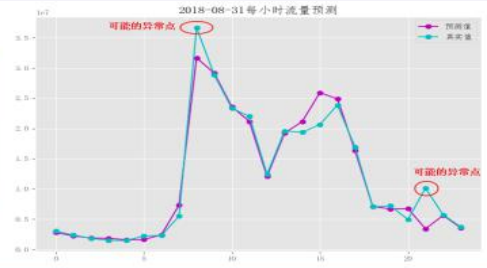
SAVE 安全智能检测引擎，在恶意软件检测方面，能够有效扫描出多种类型的恶意软件；在误报率测试中表现优异。

SAVE 安全智能检测引擎在本次测试中各项测试均达到了赛可达实验室测试认证标准，授予 SAVE 人工智能恶意文件检测引擎“东方之星”证书（SKD ZS 2018-02-11-01）。

未知异常挖掘：APT

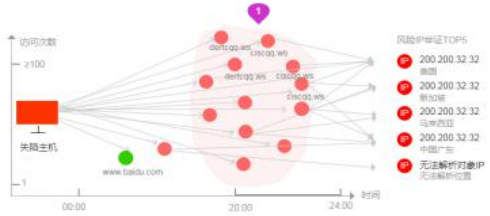
从正常的角度出发

基于基线找异常



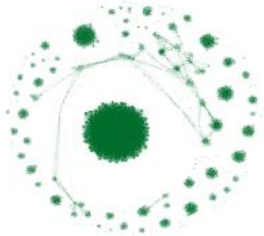
从威胁的角度出发

基于异常找异常



从横向的角度出发

基于关联找异常



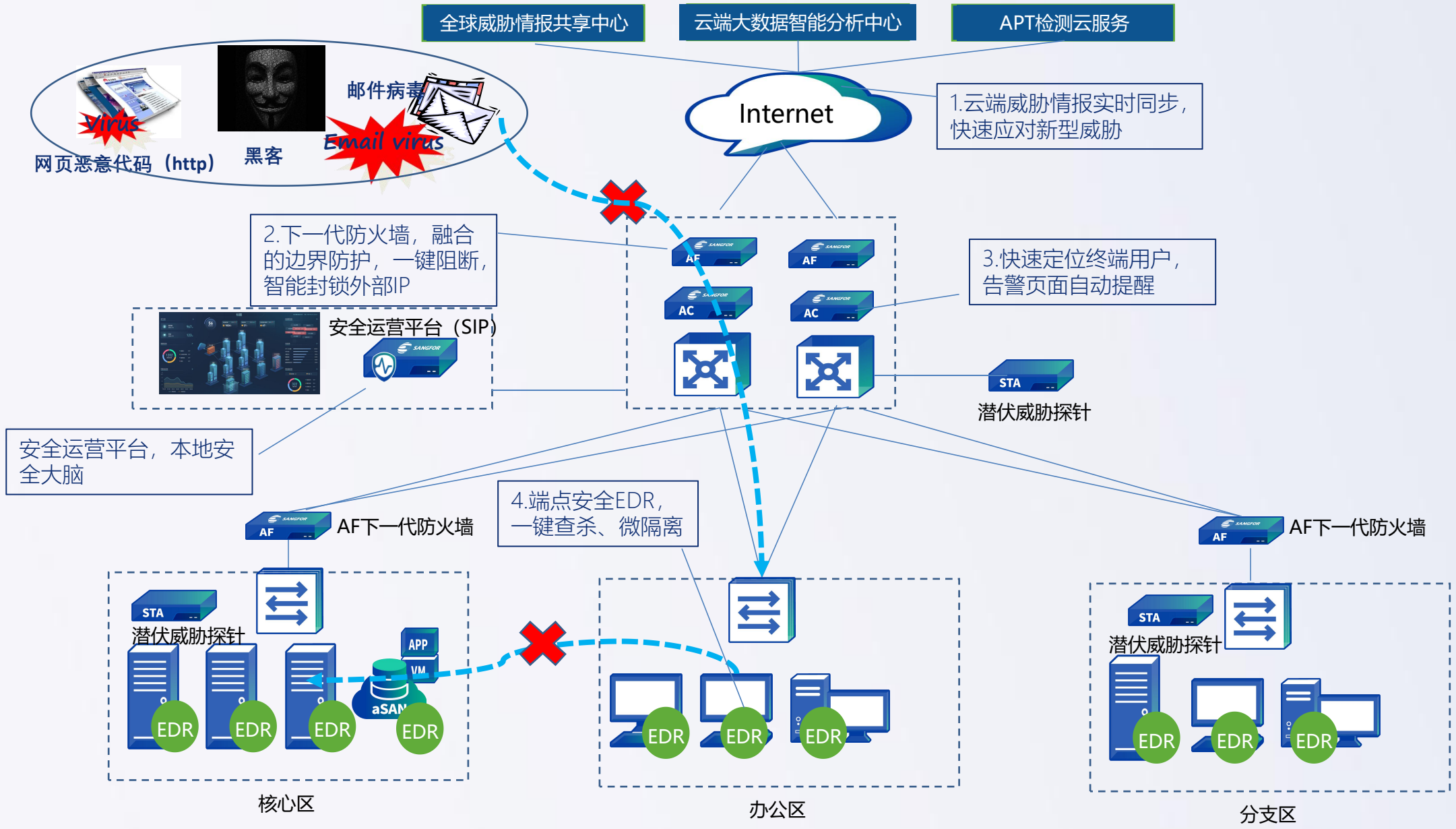
检出海莲花APT事件

在某股份制银行发现海莲花APT事件，使用IOcUYAAAAAAAAAAAAAAAAAAAAAAC-O.co.uk这样的DNS隧道传输数据

```
112.[illegible], 1, psqke49i7lxul6[illegible]7tevq56i4u8t3m78cqlcod5xmq5m3kc.me8nm4p7j8fce83xppjplsquqngewnomkbdfinppjonnm8togjks7cpnap3.dst
112.[illegible], 1, 57xdnkla8qetm8[illegible]8v25o6t2kcrxfqcqx9upmkxafvg.8vxsgae6lh4ocvl9pilr33qsohspovraw69i356tpo4ia9angp7kuqce2s4ux.fwc
112.[illegible], 1, ui2c6os985rdaw[illegible]mmlrf7l6pa39g4l9ga4c3kj8.dwhnl9a7mbg5epjfqoa7lt62bk3vi5a4o9f6ofgwjfmovitw9423pd794.3b6aib7ofair
112.[illegible], 1, 7a7nqhgiwcbvp[illegible]94t95fi3dmg9qpm7vjkb7w8.4xhrbxvubs9orgw3598q7qhxtivfd6vlbawxbsfw64xspvak6we8wtc.hwxvodd24jakjodv
112.[illegible], 1, kqfrp6p898b58q[illegible]b4fna9hxkntvbwiab7ghsxmub46.wmssh.com
112.[illegible], 1, 2b59tfaqqn8v3o[illegible]f2n9ib29ilihwg6b9vuorki.bd2fkwdikfax4hsqhudp9h6eindosvepwrjutedjdmpmv558ufdr7dhw.8xoe8qxehwtjfc
112.[illegible], 1, 4p3dcuf4txqmhs4[illegible]5inb7b5oxvk3wnjgrje2mx.cuwdnnj6d77om.wmssh.com
```

高效的协同联动响应体系

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



人机共智、自动化驱动的安全服务

人机共智构建全面安全能力
威胁情报驱动快速响应闭环
自动化提高响应效率

通过能力的扩展，帮助用户从容应对“六大安全挑战”

安全评估类服务

- 安全风险评估
- 渗透测试

咨询规划类服务

- 安全规划咨询
- 等保建设咨询
- 安全管理体系建设咨询

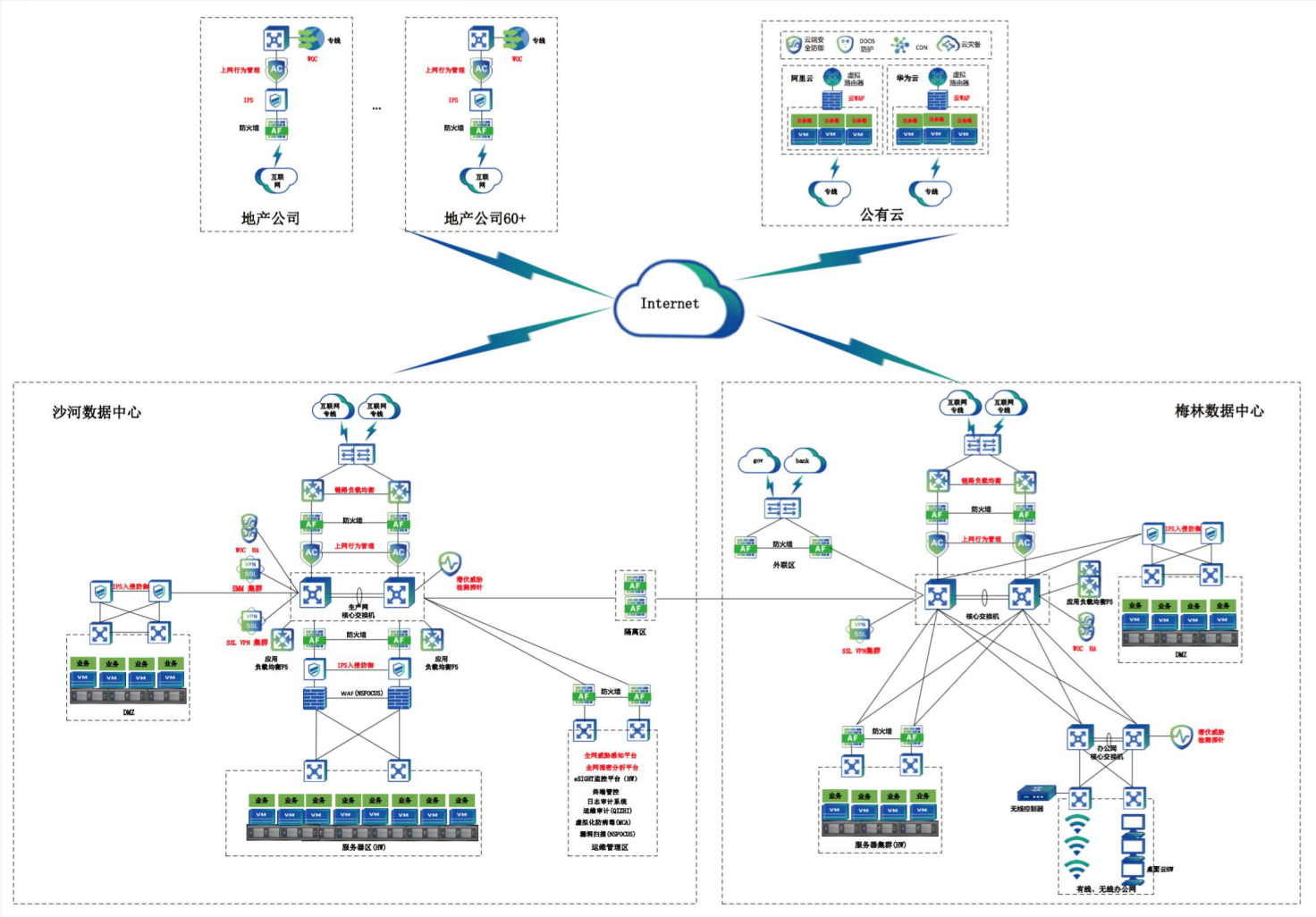
安全运营类服务

- 漏洞管理
- 威胁监测与主动响应
- 应急响应
- 应急演练

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

实践案例

万科集团整体安全加固规划



客户需求

1、地产分支安全洼地且IT能力薄弱，无法有效应对；总部经常遭受分支地产高频攻击，无法防御和明确安全责任；

2、集团信息安全不完善，边界出口、移动接入等仍旧存在薄弱环节；

3、地产敏感数据较多（代码、价格、客户信息等）难以防止外泄和溯源；业务（尤其开盘期间）实时性要求高，如何在网络侧提供高效保障。

解决方案

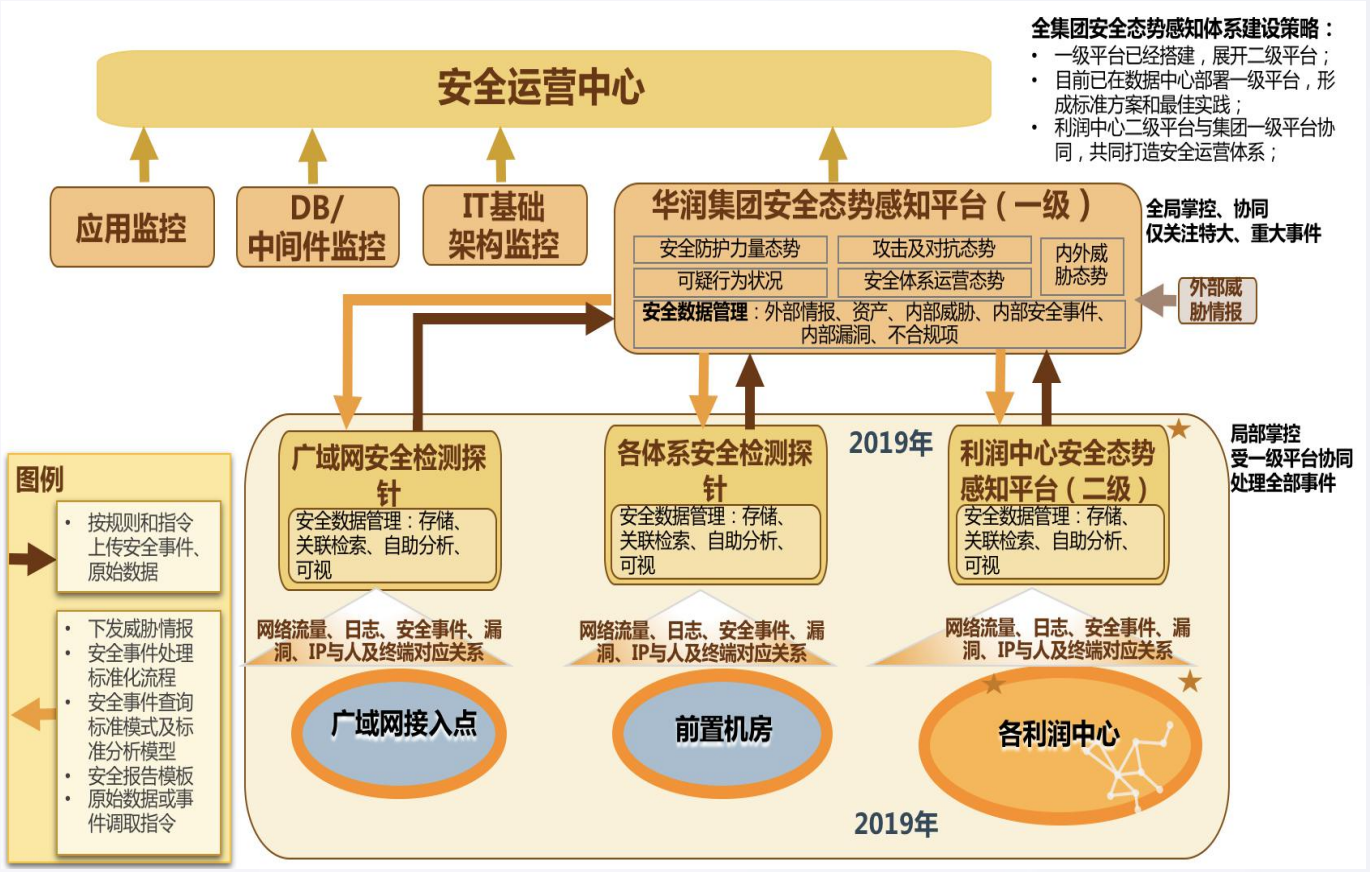
结合万科实际情况，建议建设方案思路：

1、在现有的双中心架构上，对安全建设进行体系化评估主要包含到分支安全、总部出口边界安全、移动接入安全、外发泄密分析、链路业务高可用等。

2、通过内网威胁检测+边界安全加固，帮助客户构建从“被动防御”+“应急响应”到“积极防御”+“持续响应”的闭环安全体系。

3、基于全局安全可视化技术，不仅达到安全能让领导看懂、读懂的效果，还能够让运维人员通过平台掌握总部-分支网络安全动态，快速定位及解决安全问题。

华润集团全网态势感知安全建设



一、项目背景

2019年华润集团为推动全集团智能化发展，强化集团总部IT市场化管理意识和服务意识，根据集团十三五信息化战略落地需要，为适应市场及技术发展对集团转型升级的需要。2019年华润集团信息管理部单独成立了润联科技；为全社会提供IT服务，同时需要统管全部集团体系内的建设，并成立集团层面的安全运营中心；

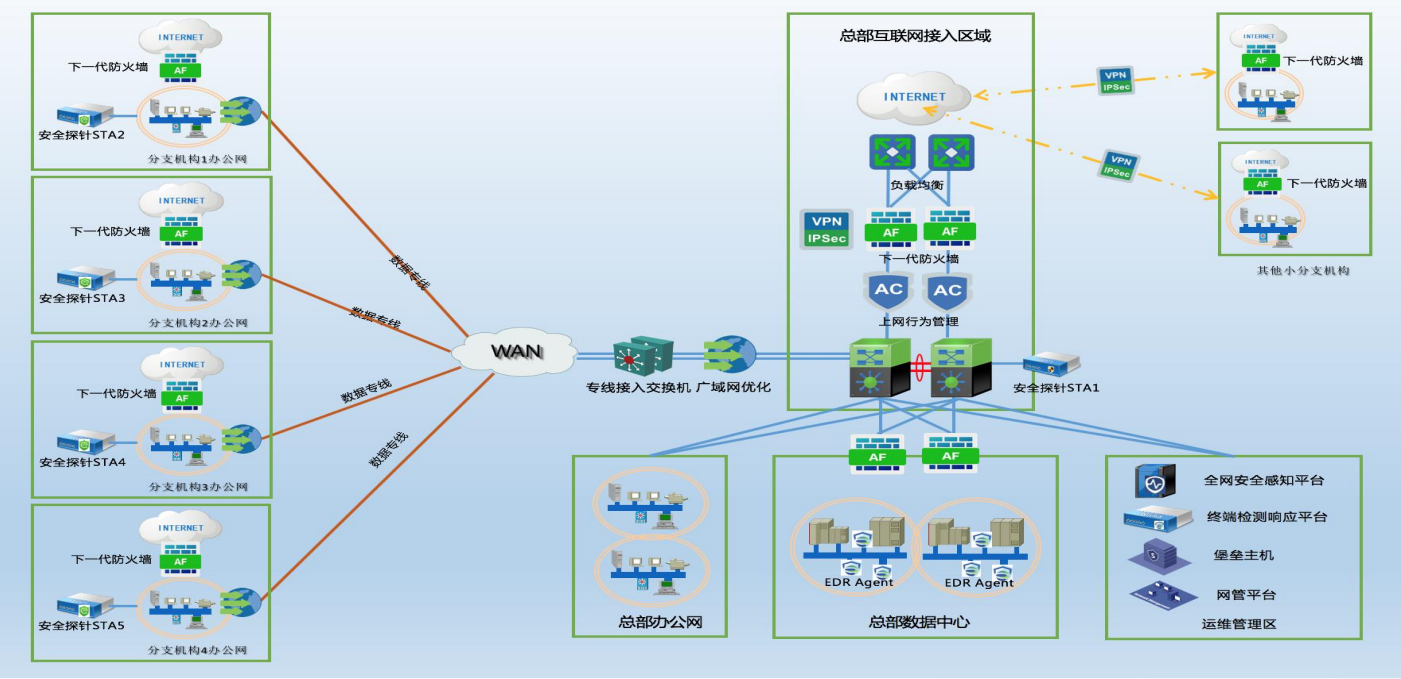
二、需求分析

1. **护网行动**：基于2020年的护网行动的关键基础设施提前建设布局
2. **安全管理**：基于润联的本身的指责：统管各个子SBU利润中心的信息化建设，多级态势感知是打通全集团的关键工具
3. **安全效果**：客户的业务高度云化，分支机构单位组织和广域网繁多复杂，存在的暴露面和风险极高。

三、方案设计

1. 通过在各利润中心的广域网接入点核心交换上部署潜伏威胁探针。在汇总关键的核心交换节点部署二级态势感知平台安全监测感知平台，实现对各利润中心办公网、数据中心安全态势的全网安全监测和全掌握。
2. 在华润集团汕尾数据中心运维管理区部署安全感知平台对华润集团汕尾数据中心各节点安全检测探针的数据进行收集；除此之外，在利润中心的核心关键节点部署二级态势感知平台，对利润中心各节点安全检测探针的数据进行收集，并通过可视化的形式呈现业务资产及针对关键业务资产的攻击与潜在威胁；同时二级平台会将分析出的安全事件等信息传输到华润集团一级平台，实现全网监测。

康佳集团整体安全加固解决方案



二、解决方案

（1）“网、端、云”安全立体防护

基于“安全云脑+AF + SIP + EDR”的新一代威胁防护架构，形成“防御、检测、响应”闭环安全体系。实现事前风险预知、事中积极防护、事后持续检测及响应。

（2）全网安全风险态势感知，降低运维的复杂度

分支通过AC+AF设备接入态势感知平台，形成全网态势感知，实时检测分支的安全风险，并结合集团信息安全管理与应急响应制度将风险缩小在可控范围之内，降低了运维的复杂度。

一、项目背景

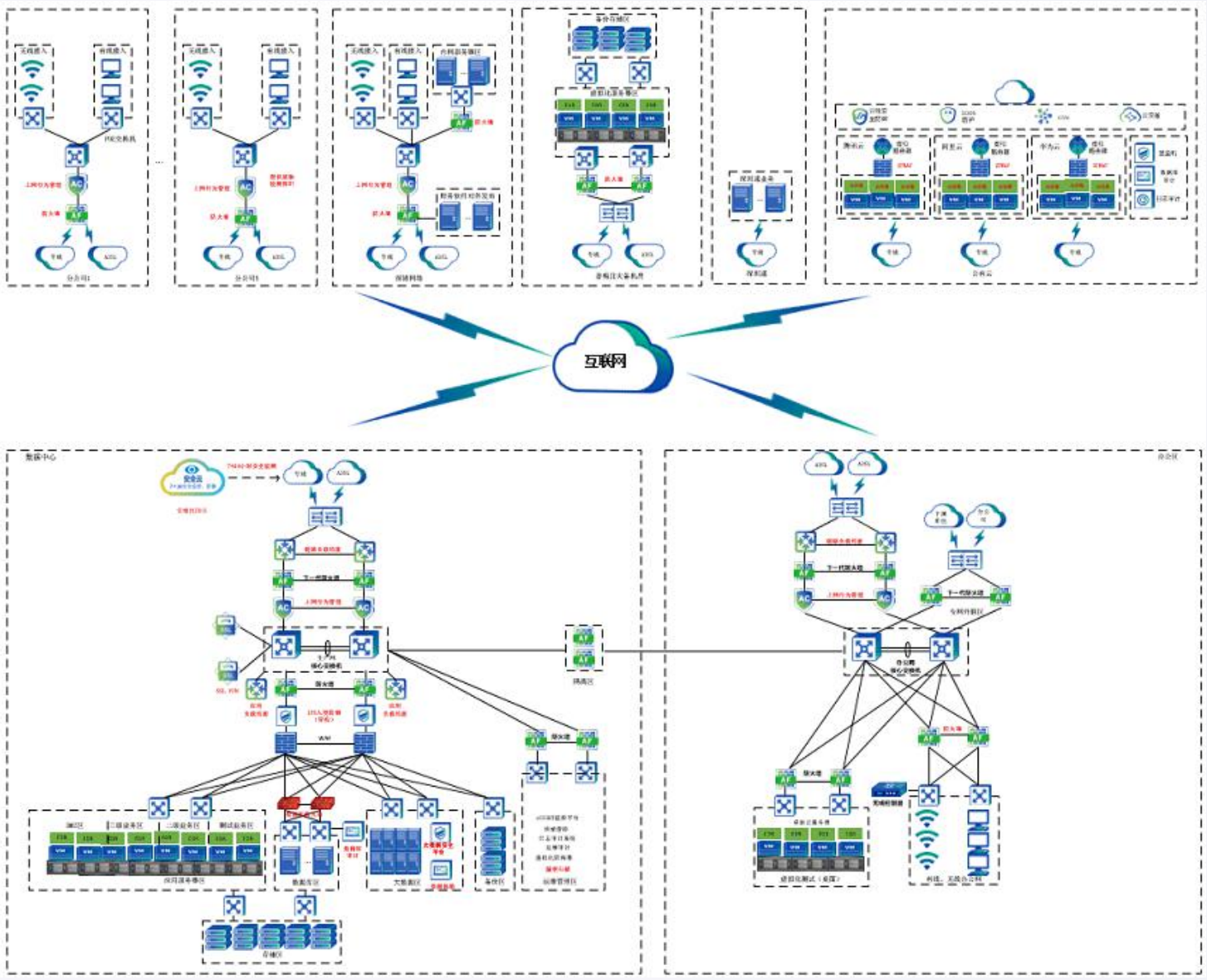
随着互联网的持续发展，当前康佳集团通过网络将总部与各分公司结合起来，便捷的沟通和共享方式大大提高了企业的生产力和工作效率，如何能够**保障一个稳定、安全、便捷的整体网络**成为IT建设的重要课题。尤其是近年来制造业爆发的安全事件层出不穷，客户非常关注网络安全体系化建设，希望有一套**先进的安全理念和安全体系化方案能满足业务发展**，保障业务开展的安全及稳定运行。

二、客户收益

整体安全方案先进、实用，凸显集团总部在网络安全示范效果。

客户着重关注智慧办公诉求，比较重视人工智能、大数据分析等新技术在网络安全层面应用。同时，客户又非常注重实用性，要求以实际安全需求出发。客户要求，即便对标行业内其他集团公司，我们的方案都不能落后。该项目的实施，使得康佳集团用户能够更深切感受到信息化带来的便捷、高效、安全，进一步**树立集团总部在网络安全层面的示范效果。**

深圳巴士集团整体安全加固方案



一、项目背景

（1）” 智慧公交“战略规划建设驱动：

（2）巴士集团打造数字平台，海量数据大集中，更需要信息安全保驾护航。

（3）满足等级保护强合规要求

二、客户问题

（1）整个网络系统规模大、结构复杂，安全建设没有体系化思路和明确方向；

（2）各个分支业务系统各自为政，与外网存在多个出口，同时分支IT力量薄弱，安全统一管理、统一决策问题亟待解决。

（3）安全现状不清晰，安全成果无展示，安全效果难预期，如何解决安全投资价值回报的问题

三、方案价值

构筑了深圳巴士集团整网安全防御，通过全方位监控，提高了网络安全防护能力和安全事件的发现和处置效率，为智慧公交的战略开展保驾护航。

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

THANK YOU