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

深信服下一代防火墙AF

主打PPT

持续进化 有效保护

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

目录

1 持续进化 有效保护

2 产品功能介绍

3 智能联动

4 产品优势及应用场景

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

持续进化 有效保护

安全事件风起云涌

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

平昌冬奥会开幕式当天，冬奥网站被攻击

2018.2

中国某军工企业被美、俄两国黑客攻击

2018.2

台积电遭到勒索病毒攻击

2018.3

医疗行业勒索事件爆发

2018.3

思科高危漏洞清明期间被利用

2018.8

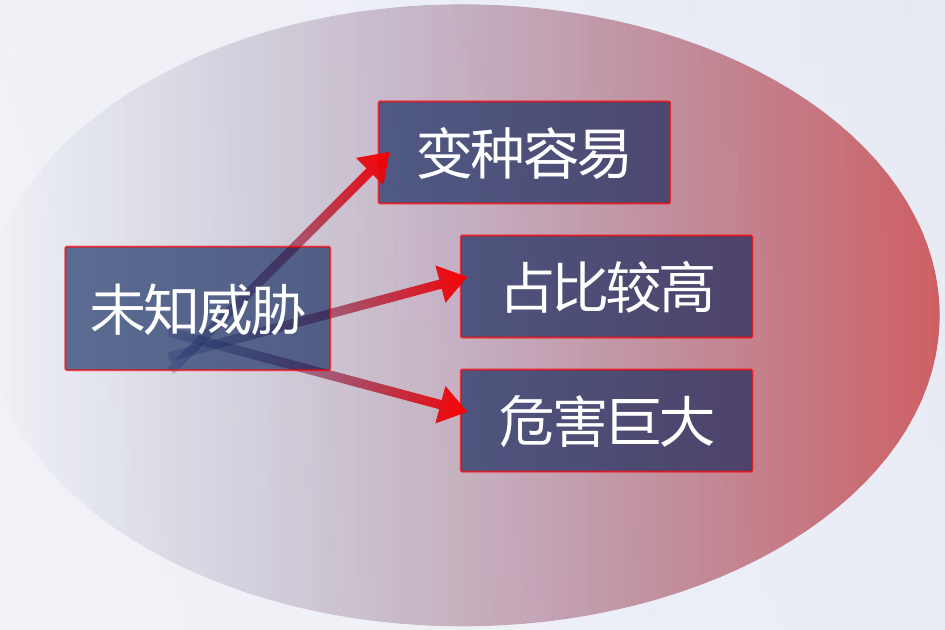
多个行业受到GlobeImposter攻击

2018.8

To Be Ccontinued

安全威胁快速进化，不断升级

安全威胁快速进化，不断升级



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

产品功能介绍

安全核心价值

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

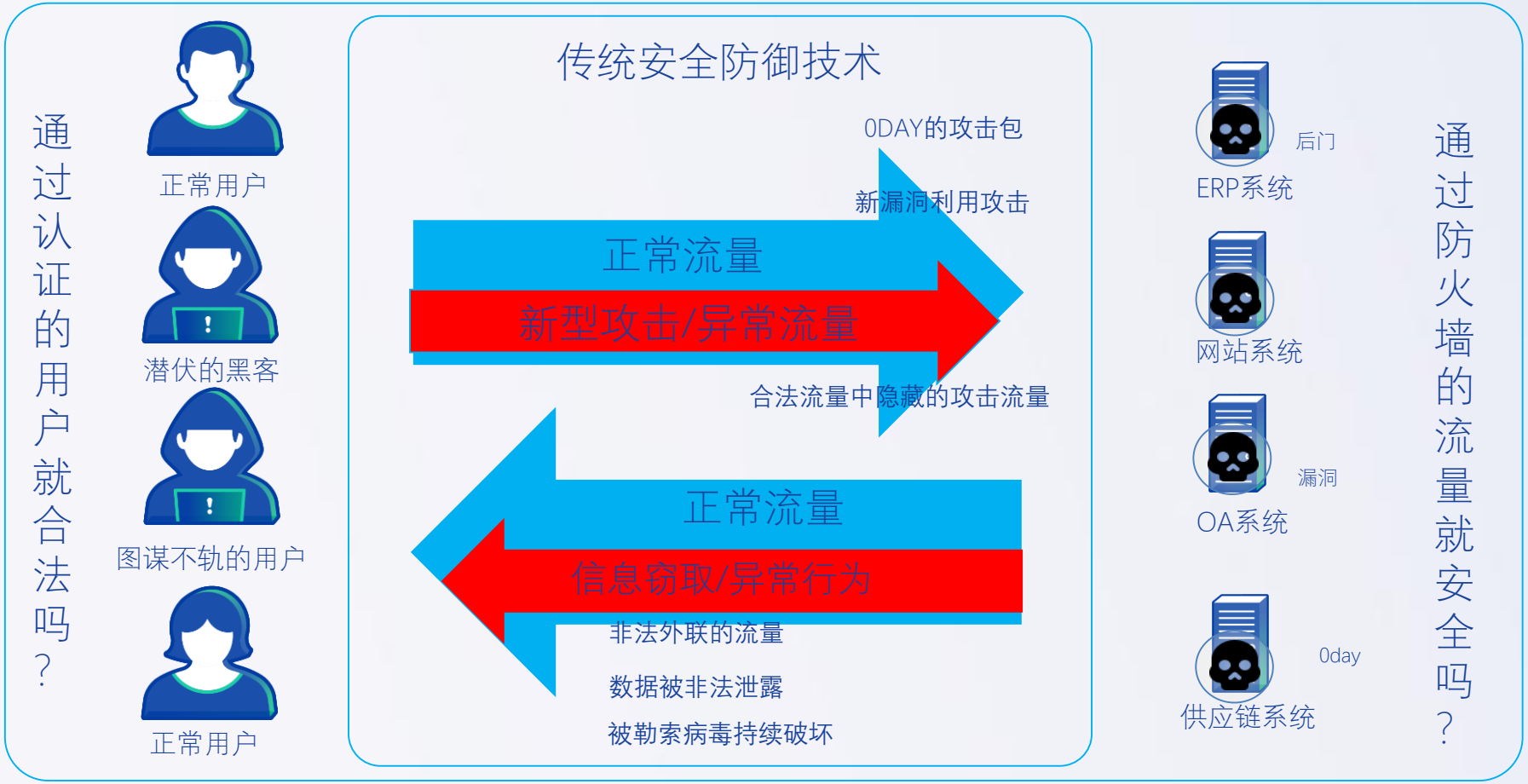
安全的基础是风险全面可视化

安全的目标是保障企业业务安全

安全的未来是抵御未知威胁

为什么需要安全可视化

看似正常的网络中，隐藏着诸多安全风险



深信服提供哪些关键的可视化安全能力

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

围绕着业务/用户安全为核心全面展示风险

业务风险全面可视

IP/端口

- 动态资产识别
- 实时漏洞分析
- 攻击事件展示
- 风险状态总览

访问行为全面可视

安全模块

- 攻击链展示：被扫描、入侵、攻击、攻陷
- 攻击类型展示：流行攻击、漏洞、病毒、未知威胁等
- 攻击举证：代码级详细举证信息

用户风险全面可视

IP/MAC

- 攻击事件展示
- 高危行为分析
- 失陷终端展示
- 风险状态总览

风险定位

数据有效分析

图形化展示

更准确的检测和防御

更高效的安全运维和风险处置

深信服的安全可视化-风险全面可视

安全的目标是保障企业业务安全

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

事前	事中	事后
预知	防御	检测 / 响应

让安全更有效、更简单

全面业务保护-事前风险预知

资产=业务　　威胁=攻击　　脆弱性=漏洞

资产识别（核心&非核心业务）
敏感信息识别（敏感页面）
实时漏洞检测（漏洞、配置、口令）
高危攻击检测（黑链、Webshell等）

……

NGAF
实时漏洞扫描

代码更新

资产识别　　**威胁识别**　　**脆弱性识别**

7*24小时实时监测核心资产、关键风险、严重漏洞

安全的目标是保障企业业务安全

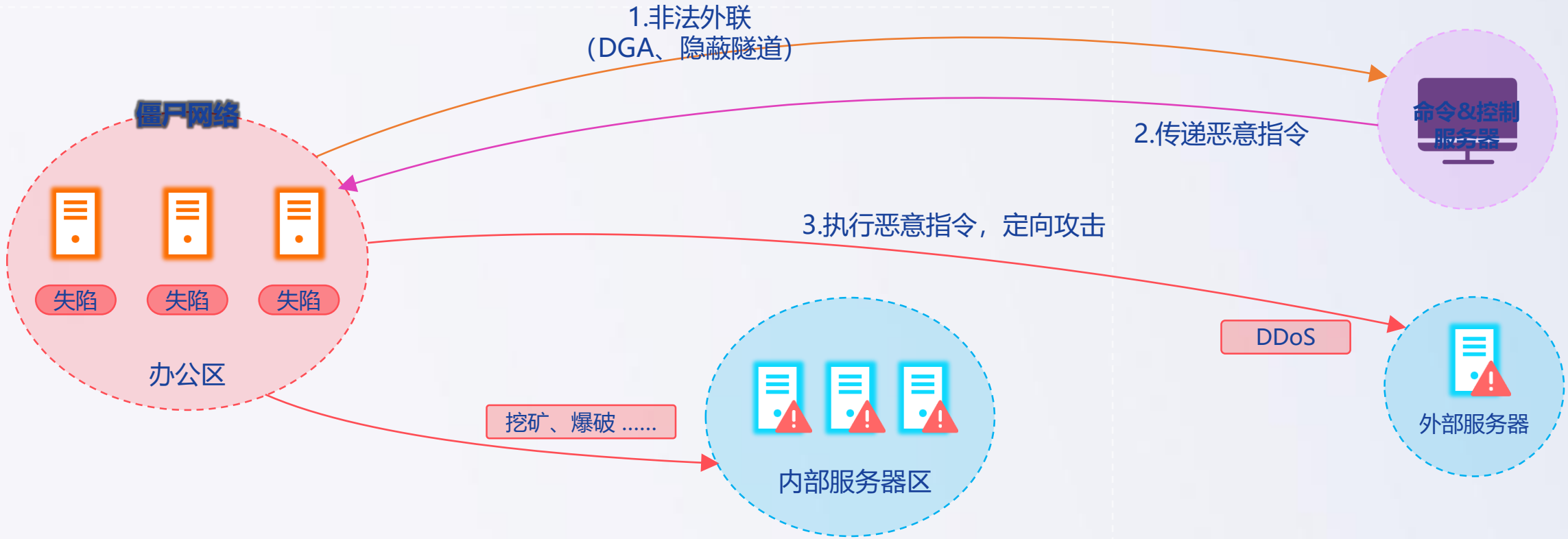
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

提供L2-L7的全面防御能力，提供专业的应用层防御能力
内部融合众多安全模块如IPS、WAF、AV、URL过滤等，精确封锁恶意威胁

深信服下一代防火墙

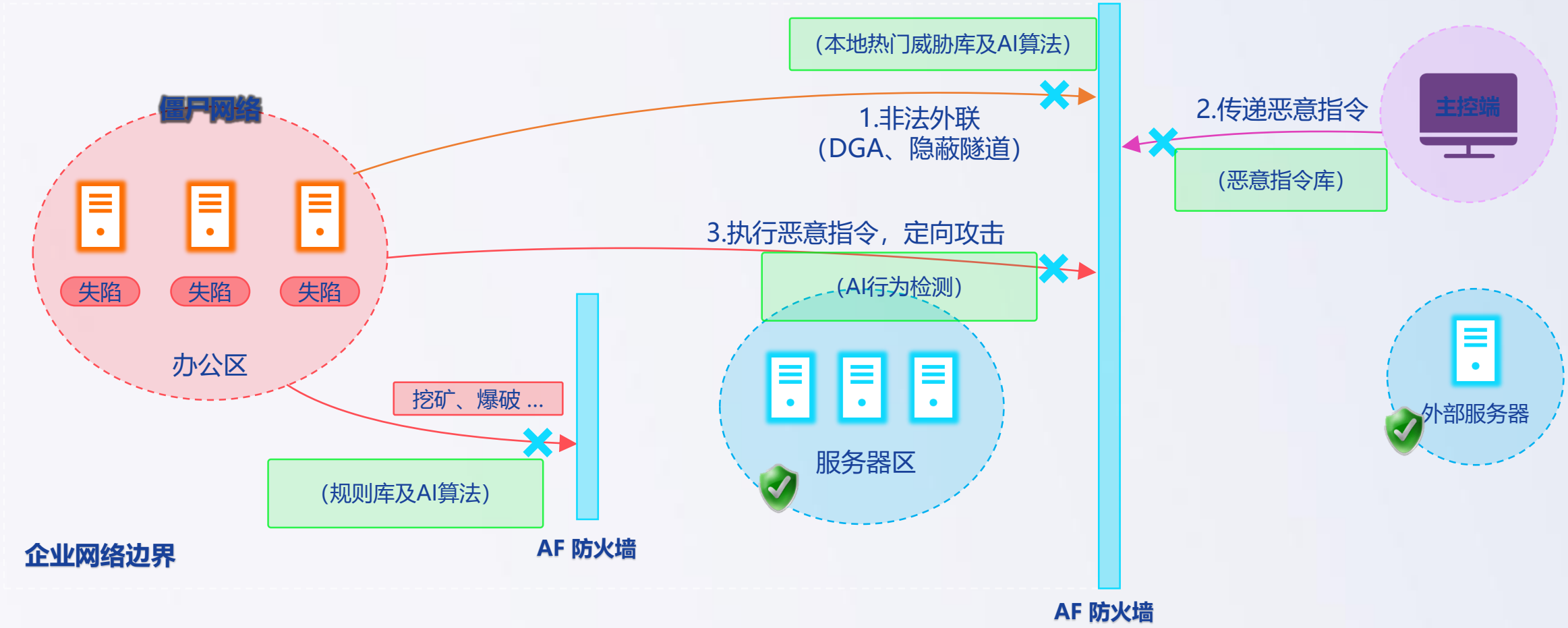
- 全球热点TOP10应用攻击及企业高危的应用层攻击，如SQL及Webshell
- 水坑、鱼叉、邮件等钓鱼攻击，勒索病毒、远控木马、异常流量等深度检测，抵御外联风险
- 细粒度内容过滤、应用识别，精细化访问控制、策略优化等机制可帮助用户将风险最小化

全面业务保护-事后持续检测与响应（以僵尸网络为例）



攻击者通过植入的黑链、Webshell及驻留在终端的恶意程序进行非法连接

全面业务保护-事后持续检测与响应（以僵尸网络为例）



全面业务保护-事后持续检测与响应（以僵尸网络为例）

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

1 风险全面感知

服务器识别

用户终端识别

敏感页面检测

漏洞风险识别

开放端口检测

2 风险综合防御

- Web应用安全防护
- 漏洞入侵防护
- 终端上网安全保护
- 勒索病毒入侵防护
- 社会工程防护
- ……

3 风险持续检测

- webshell
- 远程代码执行
- 僵尸网络
- 恶意黑链植入
- 异常流量检测
- ……

4 风险快速响应

- 安全待办事项
- 多重预警
- 一键阻断
- 应急响应
- 专杀工具

持 续 保 护

全面业务保护-事前预知-事中防御-事后检测与响应

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

何为未知威胁

未知恶意软件、病毒变种、新型病毒

利用0day漏洞的APT攻击

各种灵活多变的绕过攻击，如Struts2、Webshell

未知威胁的危害

台积电勒索病毒损失11亿

黑客盗取快递公司近亿条个人数据

医疗行业、法院受到勒索入侵

各行业网站被非法篡改

基于AI的杀毒引擎-简介

集成学习

深度神经网络

自然语言处理

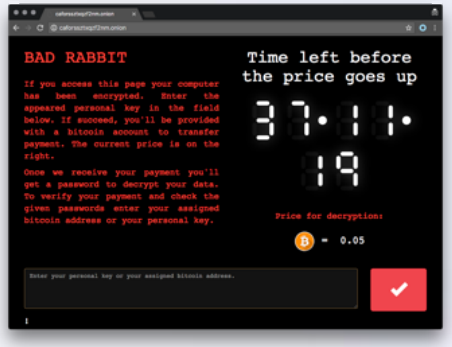
SAVE

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



Bad Rabbit（17年10月出现的最新勒索病毒），年后最新出现的 GlobeImposter 2.0 勒索病毒均能使用旧模型查杀。

基于AI的杀毒引擎-优势对比

	传统引擎	SAVE引擎
特 点	1. 固定算法 2. 人工提取特征 3. 样本收集受限	1. 人工智能算法的自我优化 2. 特征自动提取 3. 海量样本自学习
效 果	未知/勒索病毒应对乏力	✓ 有效抵御未知病毒、勒索病毒

基于AI的杀毒引擎-页面展示

抵御未知Web攻击-词法语法分析

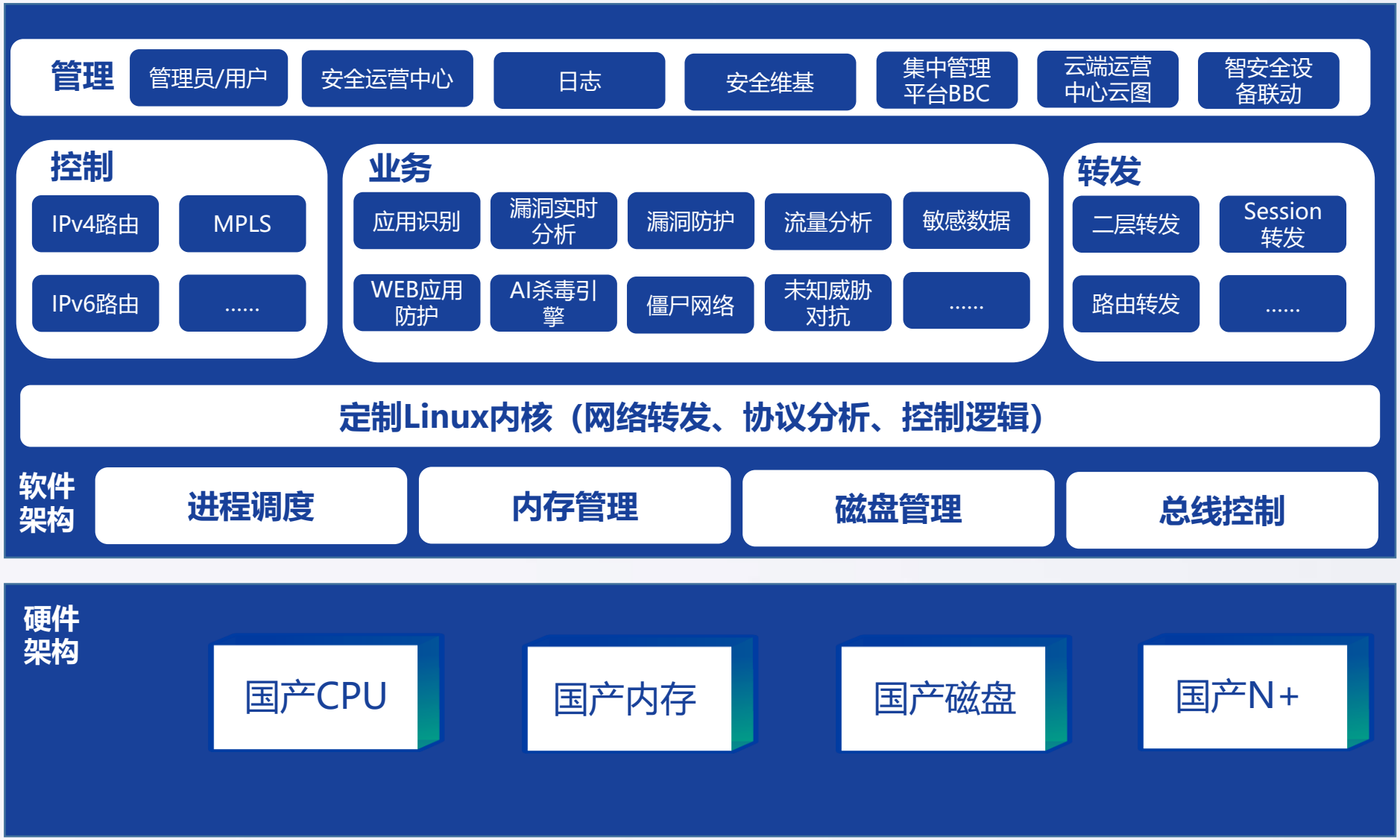
基于语义规则的原理，基于理解语言规范基础上，解析异变的web攻击，还原威胁

抵御未知Web攻击-优势对比

	传统技术	深信服web保护
特点	1. 传统规则无法抵御0day 2. 应用开发的不规范导致较高的误判率和漏判率	1. 基于语义分析抵御0day攻击 2. 深度协议解析、智能解码，以语义分析为核心，基于海量数据构建Web攻击模型，降低误判及漏判率。
效果	无法有效抵御应用层风险	✓ 全面抵御来自应用层的攻击

深信服国产防火墙

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



国产自主的安全操作系统
安全可信的专属内核
一次解析多模块处理
L2-L7层全程防护

全国产化高性能硬件架构
高带宽低延迟高速I/O
完全支持CPU虚拟化
基于硬件的数据加密

全面支持IPV6技术

全面支持IPV6环境部署：包括接口/区域配置、路由配置等网络适应性功能，支持双栈和地址转换技术。

支持核心常用的安全功能：包括僵尸网络、IPS漏洞防御、WEB应用防护等

支持IPV6协议机制：（包括但不限于Core、NDP、Autoconfig、PMTU、ICMPV6）和协议健壮性（IPv6畸形报文、ICMPv6畸形报文、其他协议畸形报文）

检测项目		检测要求	检测结果	备注
支持纯IPv6网络环境		具备	符合	无
协议一致性	IPv6 Core协议一致性	具备	符合	无
	IPv6 NDP协议一致性	具备	符合	无
	IPv6 Autoconfig协议一致性	具备	符合	无
	ICMPv6协议一致性	具备	符合	无
协议健壮性		具备	符合	无
IPv6网络环境下自身管理		具备	符合	无
支持IPv6过渡网络环境	双协议栈	可选	符合	无
	协议转换	可选	符合	无
	隧道	可选	符合	无

经检测，该产品的“下一代互联网支持”符合《信息安全技术 防火墙安全技术要求和测试评价方法 GB/T 20281—2015》中所述的有关要求。

防火墙集中管理平台

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

安全统一管理

集中配置业务保护策略，ACL、IPS、僵尸网络、内容安全、WEB安全、VPN等，全面保障业务安全

风险应急处置

在安全漏洞爆发或热点威胁爆发后，自定义安全规则并统一更新进行防护

远程分支管理

网络设备配置统一下发
分支设备版本/系统统一升级
分支设备简易部署，快速上线

深信服AF产品系列


1600W
800W
200W
5.5Gbps
20Gbps
80Gbps
AF-2000-J448
2U，8个接口扩展槽位，双电源
吞吐：80Gbps
并发：1600万
AF-2000-J444
2U，8个接口扩展槽位，双电源
吞吐：40Gbps
并发：1200万
AF-2000-I482
2U，4个接口扩展槽位，双电源
吞吐：20Gbps
并发：800万
AF-1000-G640
1U，2个接口扩展槽位，双电源
吞吐：10Gbps
并发：220万
AF-L4670
1U，1个接口扩展槽位，单电源
吞吐：8Gbps
并发：200万
AF-L4478
1U，1个接口扩展槽位，双电源
吞吐：5.5Gbps
并发：200万

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

智能联动

智能联动图谱

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

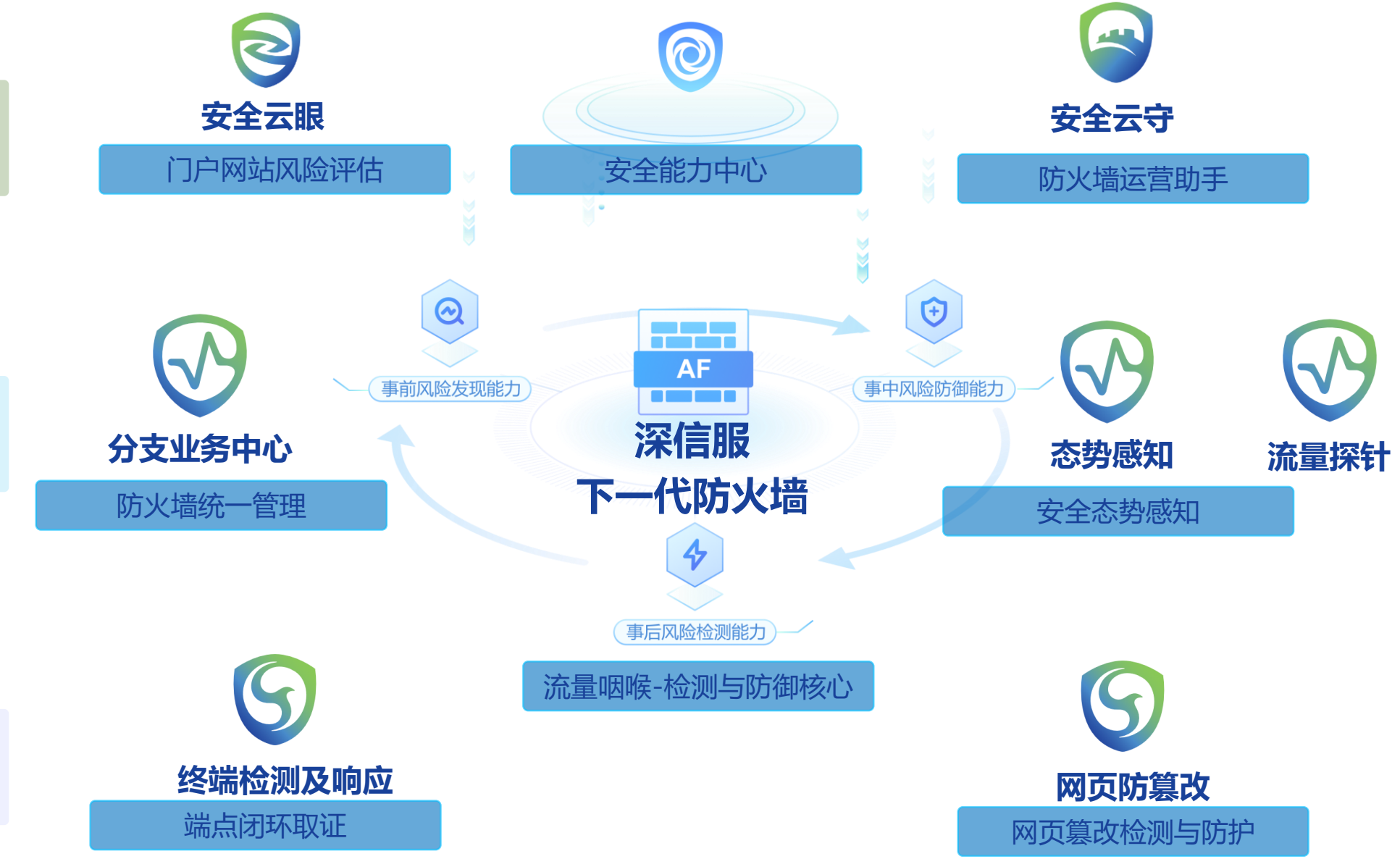
云端订阅服务

+

网络纵深防御

+

端点闭环保护



云端智能检测-威胁情报

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

威胁情报

情报共享
实时云网协同

热点情报
5min全球发布

云端安全能力赋能

抵御0day
漏洞预警防护

下一代防火墙AF

响应速度变快

- 热门威胁5分钟响应
- 全球热点事件应急响应
- 云网协同，安全能力随需扩展

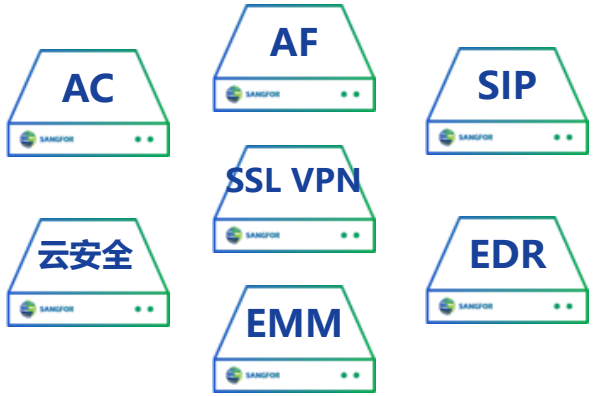
安全能力增强

规则	算法	事件
安全威胁情报	安全分析能力	IOC事件库
安全规则更新	未知威胁防护	热门威胁事件库

云端智能检测-威胁情报

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

沙箱、蜜罐及联动产品生态



暗网、社区，漏洞平台获取

暗网
ThreatPost
Hat+
0x00sec
HackForums
GraySec
AntiChat
SecurityIntell

全球厂商情报交换

网络安全威胁信息共享平台
CNVD
火绒安全 www.huorong.cn
Avira
JIANGMIN 江民科技
virustotal
RISING 瑞星

多层情报提纯

基础情报库

僵尸网络库 | 恶意链接库 | 文件样本库

单库泛化

基于已知的情报库进行攻击预测

跨库深度关联分析

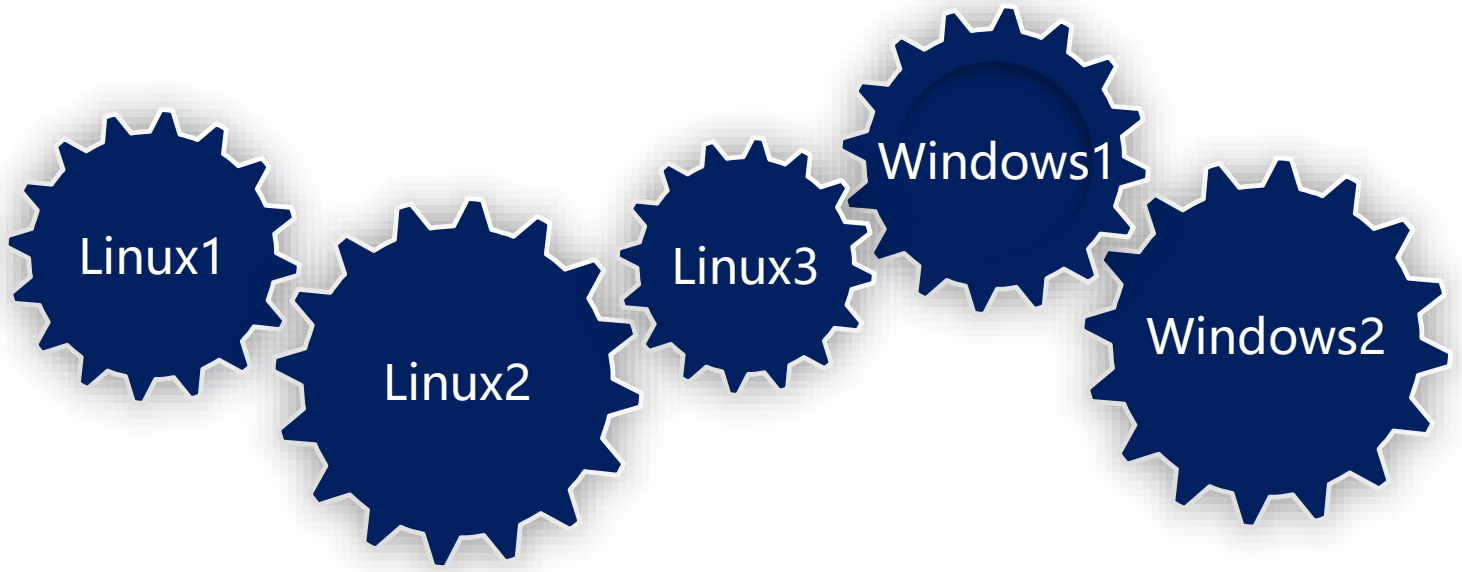
恶意样本的行为分析和异常流量检测

Spark | kafka A distributed streaming platform | HIVE | hadoop | HBASE | elasticsearch | redis | kibana

云端智能检测-云端沙箱

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

云端沙箱



主流环境完整支持的沙箱阵列

基于资源状态的虚拟环境智能调度

文件行为 / 进程行为 / 网络行为	驱动级行为监控
原始日志 / 行为描述 / 运行时流量 / 取证截图	完善的取证系统

全面覆盖的样本类型：执行类、文本来等多达近百种文件类型

业界领航的沙箱技术：反逃逸、驱动层监控、完整进程链追踪

安全云眼-门户网站全面保护

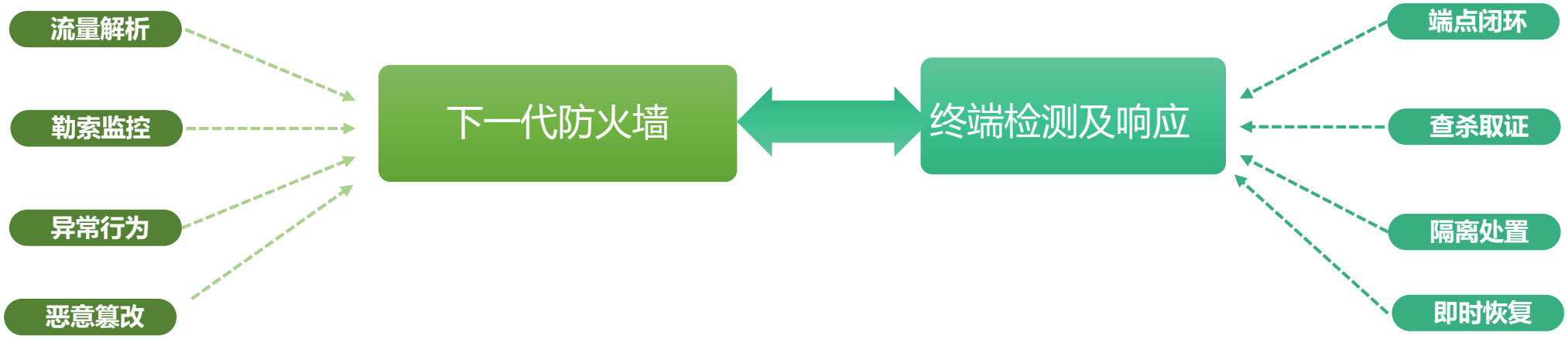
门户网站保护：通过边界+云端+终端的协同联动，对企业门户网站进行立体化纵深防护；

事前：对门户网站进行风险监测，基于云端庞大的漏洞库，对高危漏洞进行扫描、评估

事中：对web攻击及恶意扫描行为进行防御，有效抵御外部的web攻击

事后：通过边界与端点协同联动有效发现端点侧的非法篡改行为，防止网站被非法篡改

终端检测及响应-威胁闭环处置



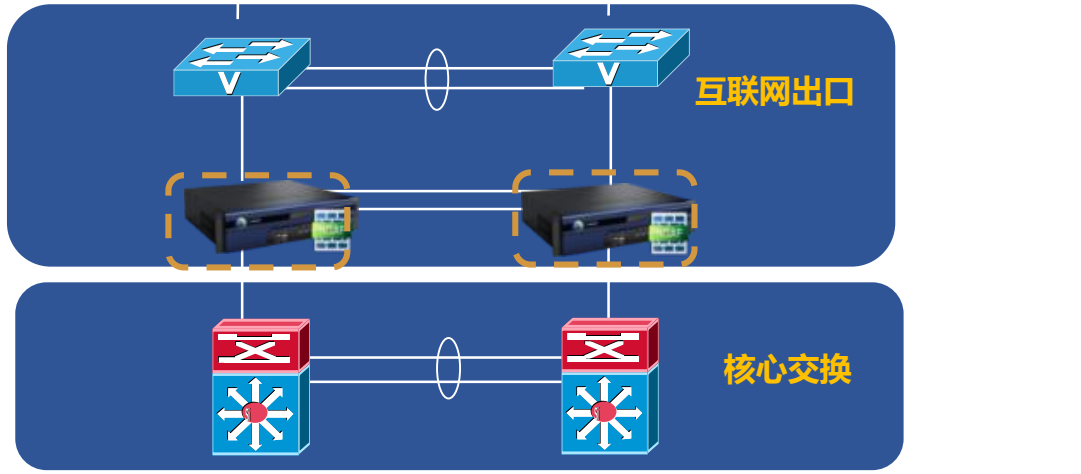
基于现网大量的安全风险，通过网络及端点深度联动提升整体安全能力，AF可以基于流量定位内网系统中的病毒、木马、恶意软件等失陷终端。通过联动EDR在OS内核及终端应用侧进行深度扫描、取证、查杀，可有效在终端侧对威胁进行闭环处置。

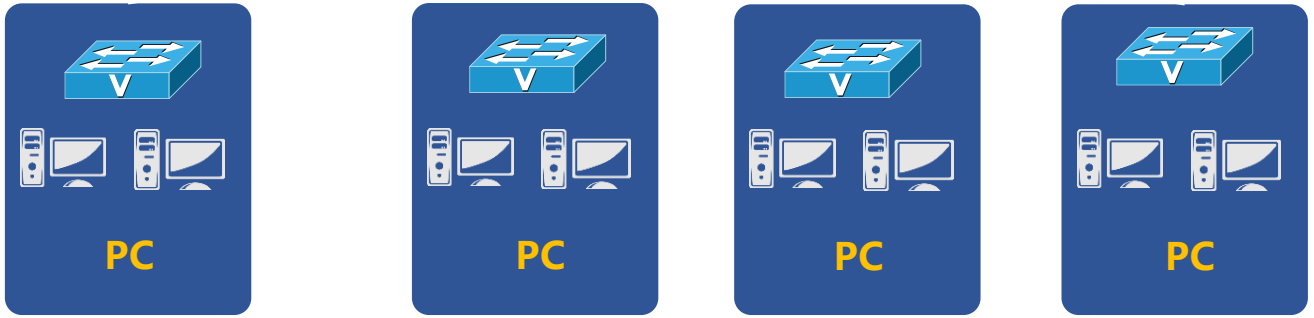
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

产品优势及应用场景

互联网出口安全防护场景

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





二、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

三、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

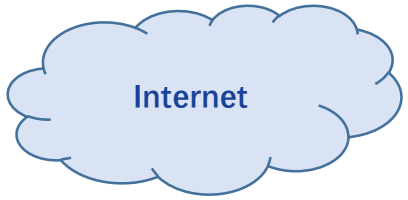
四、基于业务和用户的漏洞攻击防御

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

五、未知威胁防御

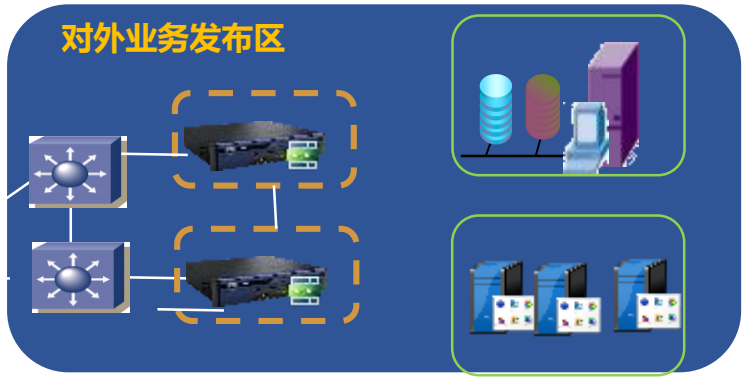
1、通过外部情报定位未知威胁
2、云端沙箱监控恶意威胁行为，深度取证
3、海量日志关联分析，热点威胁防患于未然
4、应急响应，专杀工具，高效闭环风险

对外业务发布安全防护场景



互联网出口

核心交换



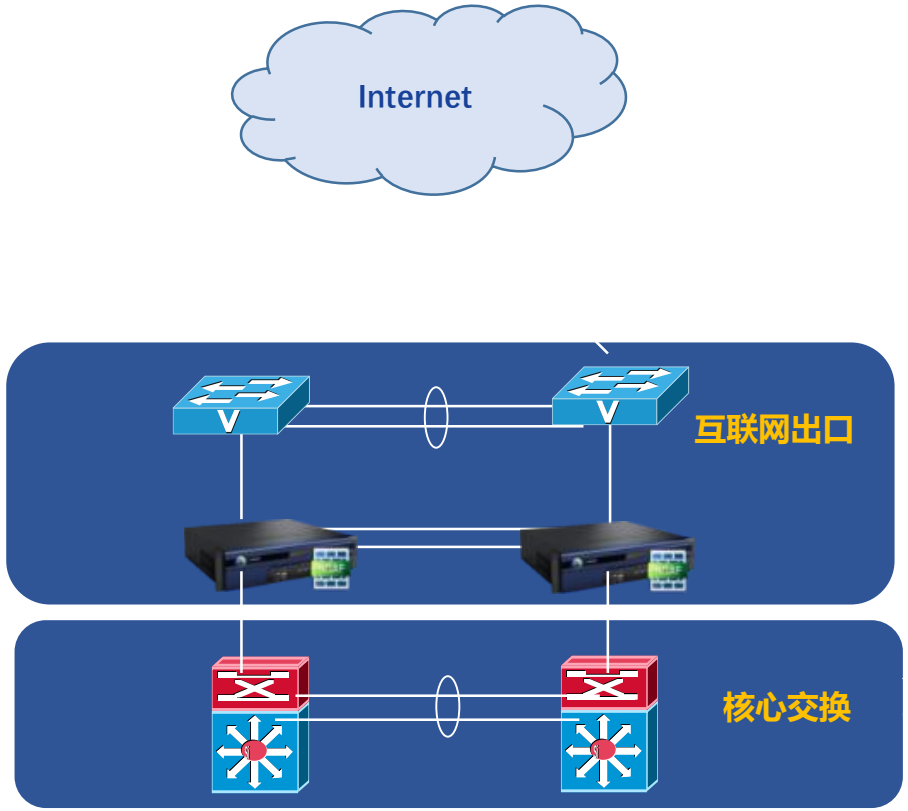
一、业务风险全面感知
1、业务资产识别
2、业务漏洞全面扫描及分析
3、业务安全状况及安全策略有效性评估
4、待办WEB安全风险一键处理

二、Web应用深度防护
1、防SQL注入、XSS、CSRF等攻击
2、防止恶意植入黑链
3、防止植入WEBSHELL
4、防止网页被非法篡改
5、防止路径非法遍历/防恶意扫描

三、Web应用合规保护
1、敏感信息泄露防护
2、HTTP异常协议检测
3、文件上传/下载控制

四、未知WEB威胁防御
1、基于正则匹配、词法语法应对众多web变种，有效降低误判、漏判
2、基于情报和沙箱基于流量上下文定位未知威胁

数据中心安全防护场景



一、细粒度的访问控制

1、在最小化原则下，基于IP、端口、协议传统五元组扩展user-id、app-id、content-id、business-id、data-id细粒度控制风险暴露

二、业务排障及策略优化

1、模拟策略匹配方式，基于业务实际状况调整网络策略，在业务异常时有效排障

2、策略优化，可以对失效的策略进行检测，如策略冗余、策略长时间未匹配、策略超过生命周期等，调整ACL控制结构。

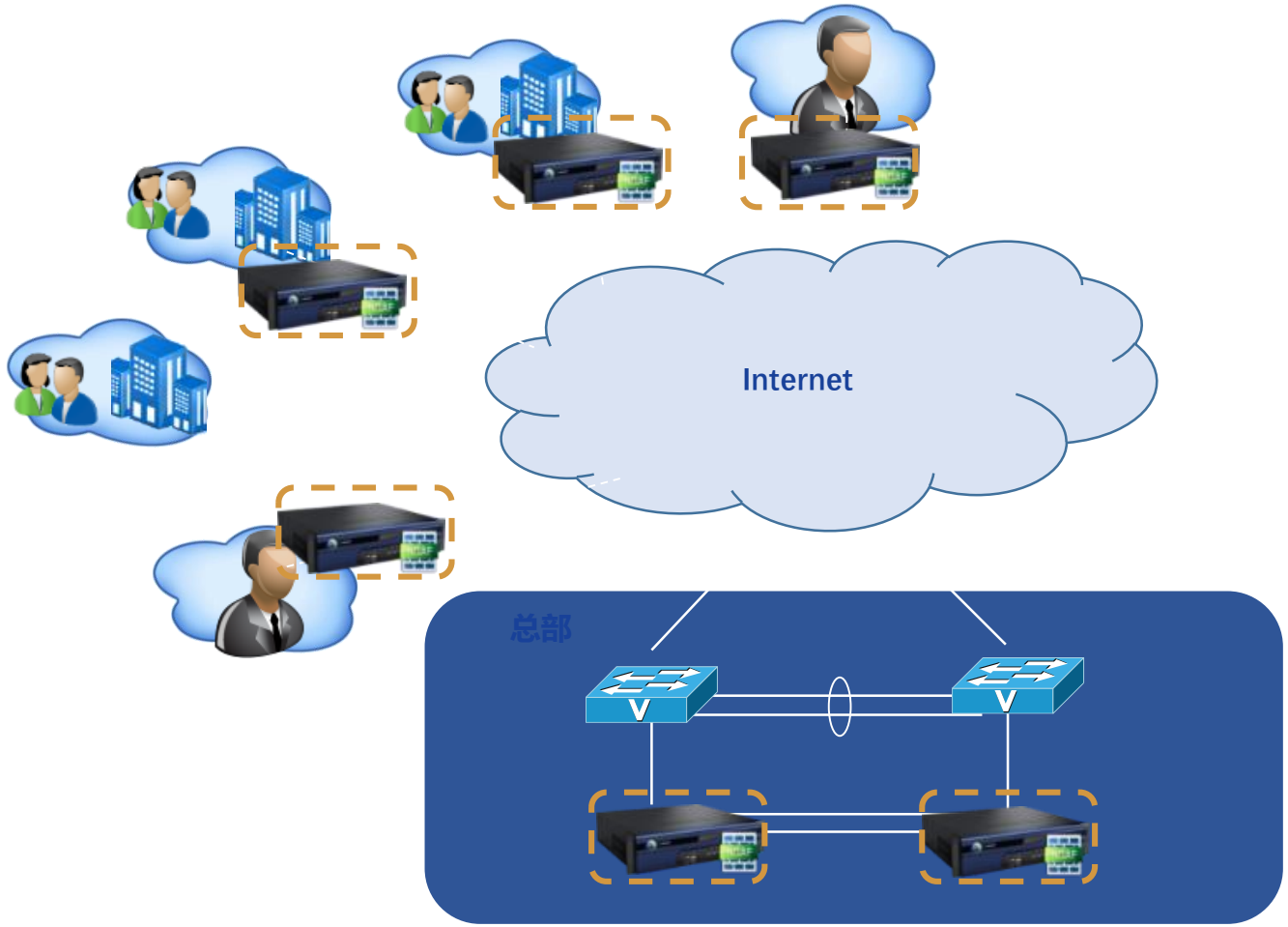
三、安全可视化及简单易用

1、对特定安全域的业务和主机进行事前-事中-事后的全面可视化，展示攻击链，对内部威胁进行溯源及取证

四、内网异常全面检测

1、异常协议检测、异常流量检测、高级攻击逃逸检测、恶意文件、CC外联、黑链检测等

分支机构安全防护场景



一、分支机构统一管理及运维

1、统一配置业务保护策略，包括但不限于ACL、IPS、僵尸网络、内容安全、WEB应用防护，保障业务安全；
2、统一对分公司设备进行版本/系统升级；
3、智能监控、智能告警、风险集中展示

二、分支机构安全防御

1、僵木蠕防护
2、勒索/挖矿/未知病毒防护
3、静态攻击代发防护
4、主机失陷防护
5、自定义安全规则统一下发，应急响应

三、智能组网

1、支持IPSEC VPN/SSL VPN
2、支持SD-WAN智能选路功能
3、基于邮件链接，一键配置实现系统分钟级上线

四、全网安全态势感知

1、分支端威胁全局展示
2、基于威胁地图进行攻击溯源

深信服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）

效益与价值：更有效、更简单

应用价值

更有效

- 全过程的保护：提供风险认知、积极防御、持续检测、快速响应全过程的融合
- 更有效的防御：网络层、应用层、新型威胁、0day等威胁的融合，消除防御短板
- 事后持续检测：绕过防御还能持续检测，如异常行为、潜伏威胁、安全事件
- 持续融合新技术：结合沙箱、情报等手段，持续提供应对新风险的能力

更简单

- 融合安全：防御、检测、响应的融合，简化安全运营的全过程
- 全程可视：全面提升安全保护整个过程的认知能力
- 运营简单：安全运营中心，仅需管理统一平台即可闭环保护的过程
- 集约管理：减少设备的部署，降低单点故障，获得最大投资回报

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

THANK YOU

2019 深信服科技