SANGFOR
深信服科技

如何应对开放业务
对数据中心带来的挑战

安全BU 王帆

SANGFOR
深信服科技

互联网+时代

数据中心业务更加开放

SANGFOR
深信服科技

开放的业务

挑战传统安全体系

SANGFOR
深信服科技

黑客被黑背后的故事

Hacking Team 400+G资料在网上泄露

管理员电脑
感染病毒

通过病毒
获取跳板

互联网和内网
从同一终端访问

通过互联网
入侵内网

数据明文
传输和存储

监听数据、获
取口令

身份认证仅使用
用户名/密码

黑客通过口令
获取服务器权限

未分析审计数据
看不见系统异常

黑客长期潜伏
获取数据

SANGFOR
深信服科技

给我们的启示

1. 外网的边界防御并不是坚不可摧，黑客可以通过各类边界进入到内网
2. 边界被突破之后，黑客几乎可以在内网为所欲为，因为内网被默认为可信域
3. 并不是所有的合法用户都在做合法的事情，有可能合法用户已经被黑客所控制

SANGFOR
深信服科技

但企业应对数据中心变化
并没有改变安全建设的思路

以“边界、安全域”为主的防护思路

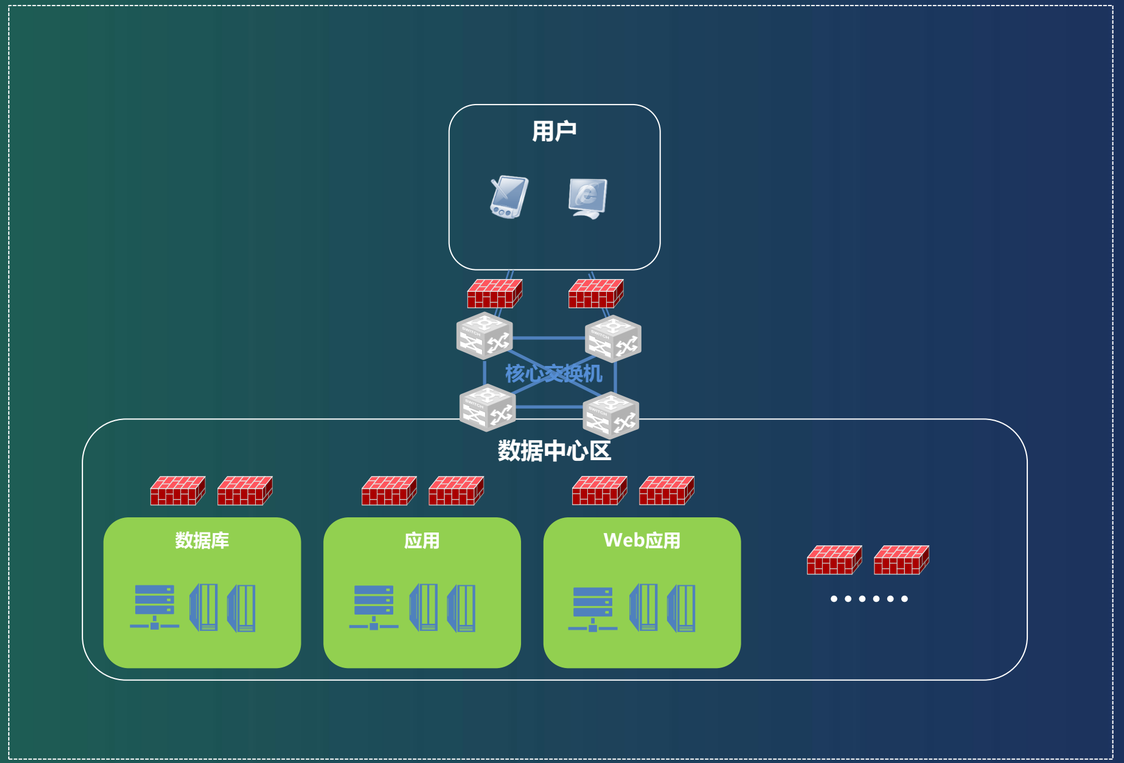
被动、防御型的技术手段

基于IP/端口/特征的运维管理

SANGFOR
深信服科技

传统安全防御

仅仅是数据中心安全的基础



SANGFOR
深信服科技

重新审视
数据中心安全

假设边界已经被突破

需要重视内网的持续检测

假设所有用户都不可信

对重要资产和用户持续追踪

就像机场安保
1、对所有进入人员在多重认证；
2、对进入的人员在机场所做的行为进行持续的追踪

SANGFOR
深信服科技

基于两个假设
数据中心安全新思路

除了传统的边界防御之外

看清用户访问数据中心业务资产的各类行为

持续对已进入内网的安全风险进行持续的检测

接入核心的业务系统的用户进行更强的认证

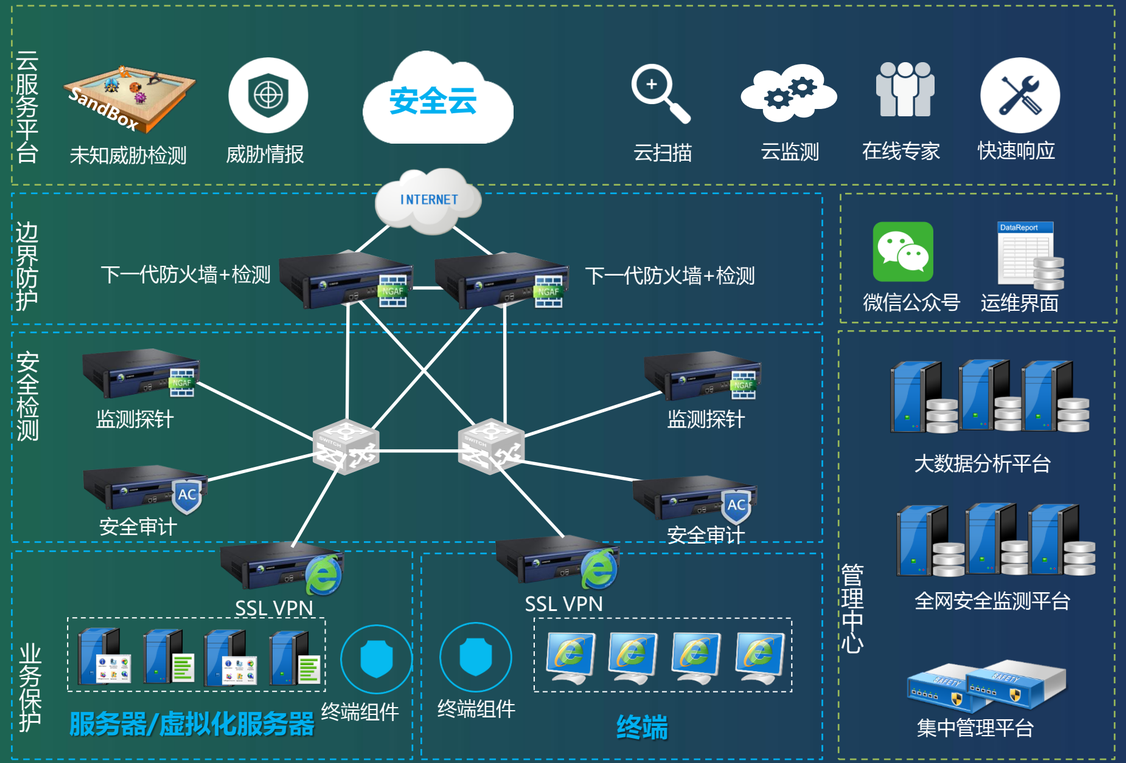
通过大数据审计访问到数据中心的所有行为

SANGFOR
深信服科技

互联网+时代
数据中心的安全建设

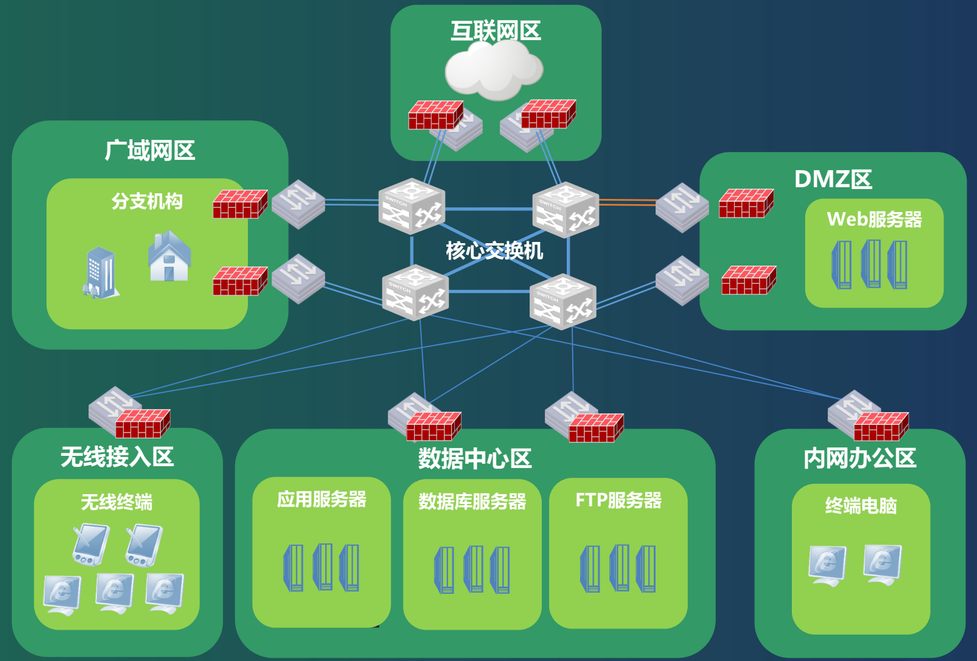
SANGFOR
深信服科技

数据中心安全建设
方案架构



SANGFOR
深信服科技

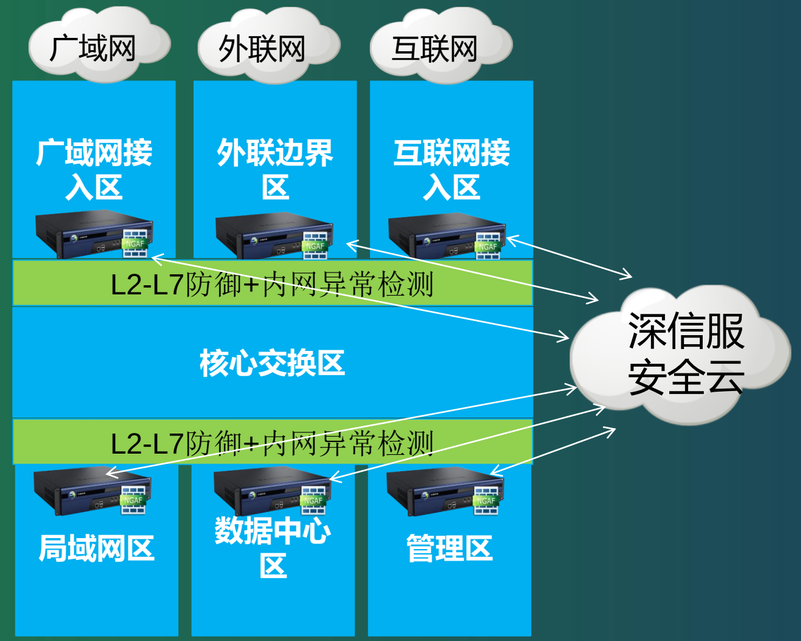
1、简化数据中心安全边界防御



阻止黑客在进入数据中心前的尝试攻击，提升黑客攻击成本

SANGFOR
深信服科技

更精简的边界安全架构



精简的安全架构：
融合：融合FW、IPS、WAF、AV
性能：单次解析架构
扩展：负载均衡对防火墙集群

防御+检测，全面识别风险：
内网攻击链检测
失陷主机、终端检测
数据外发、网页篡改、黑链检测

云端专业服务快速响应：
外部社工库，及时预警
7*24小时专家团队应急响应

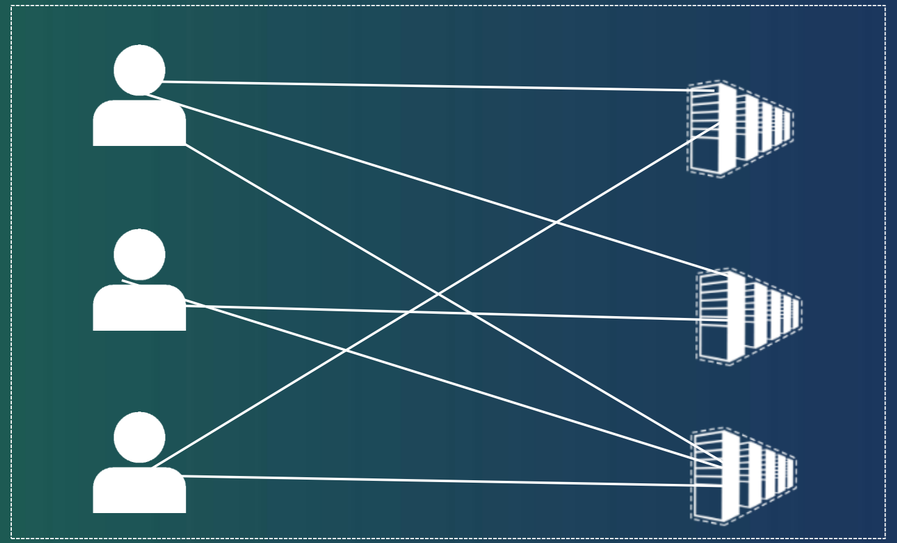
SANGFOR
深信服科技

2、可视化是数据中心的安全基础

南北向　　东西向　　多数据中心

SANGFOR
深信服科技

用户
资产访问关系可视



用户-资产的关系可视化：

1、同步用户认证信息
2、手工配置资产
3、主动发现资产
4、自动同步资产信息
5、用户与资产的访问关系

SANGFOR
深信服科技

看清用户、行为、业务资产的全风险

SANGFOR
深信服科技

3、数据中心内外部增加持续检测技术

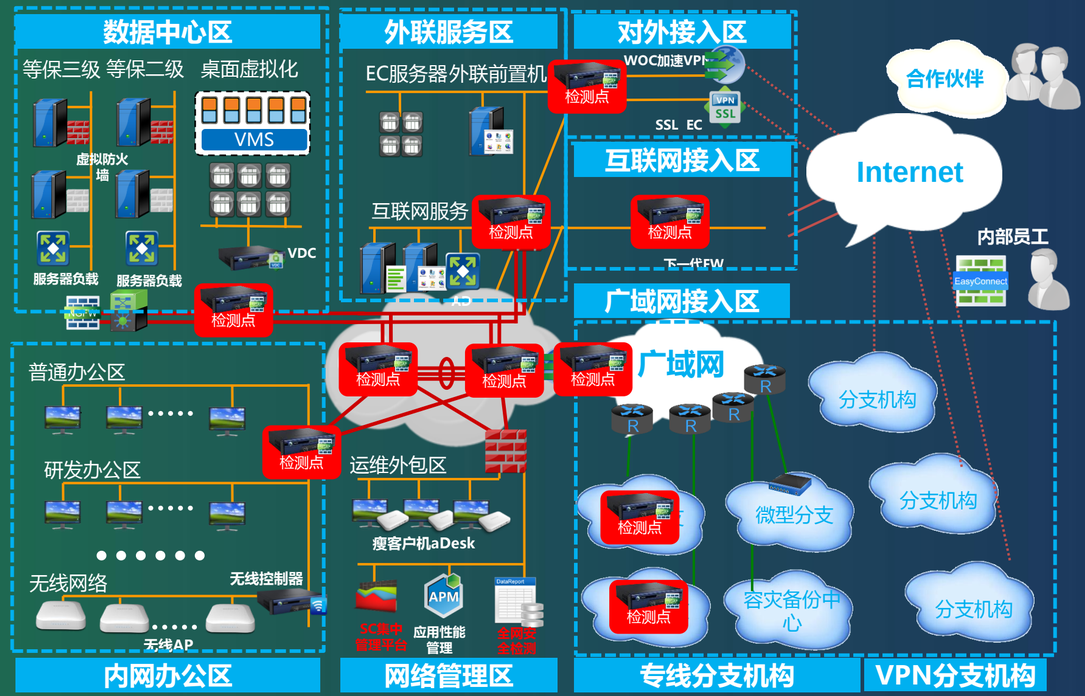
异常服务器端的检测技术

检测技术

端口/服务扫描检测	账号密码爆破	服务器向外RDP请求	网页被篡改
IP扫描检测	Web攻击检测	服务器向外SSH请求	网页存在黑链
漏洞扫描检测	应用漏洞攻击检测	主动外发DNS异常链接	网页存在黑链
弱密码扫描	漏洞攻击检测	webshell上传检测	批量登陆异常
威胁情报收集	缓冲区溢出检测	内网进行扫描	数据库异常访问
	跳板攻击检测	内网dos攻击	
	僵尸木马检测	内网入侵攻击行为	

SANGFOR
深信服科技

3、数据中心内外部增加持续检测技术



四个检测点

1、外联边界
2、数据中心
3、局域网核心
4、广域网边界

两种检测方式

1、下一代防火墙开启检测模块
2、旁路部署检测探针

SANGFOR
深信服科技

4、重要业务系统安全加固

安全接入

安全域最小化

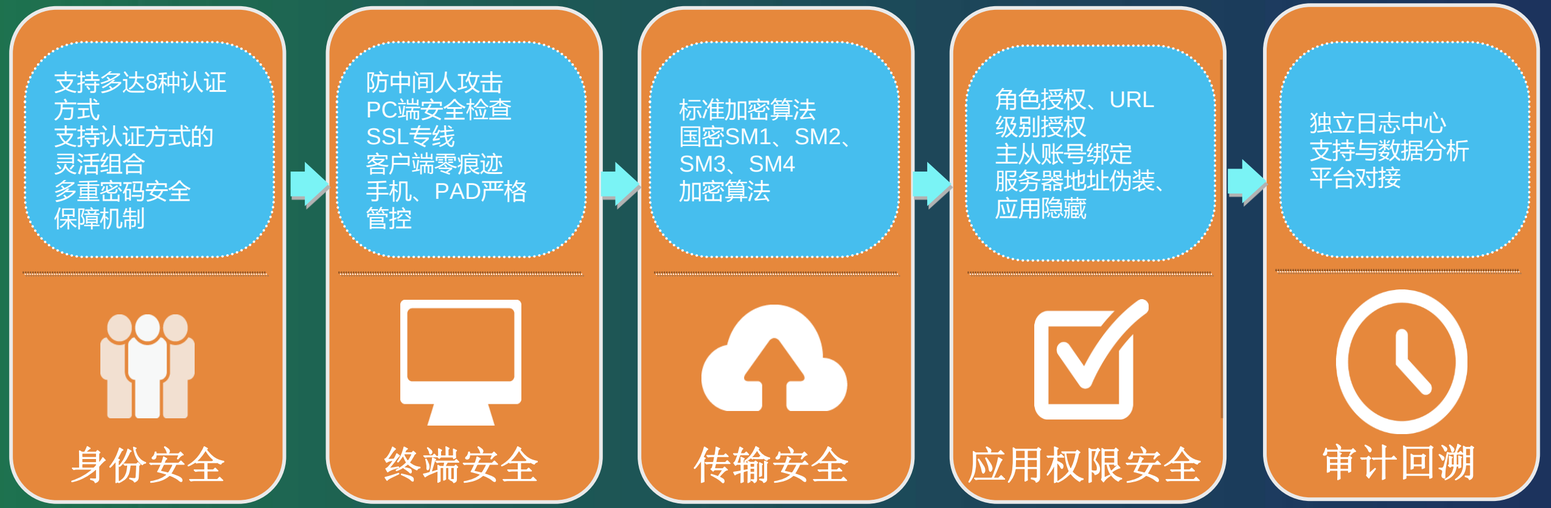
SANGFOR
深信服科技

核心业务系统安全接入

- 合法的用户和终端
- 合法的权限和行为
- 全程数据传输加密
- 全程记录回溯

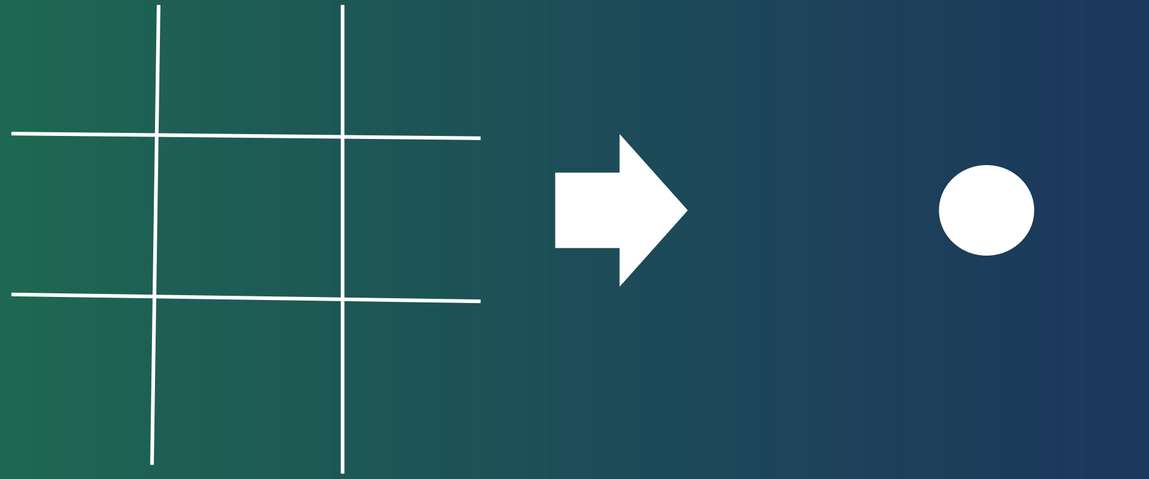
SANGFOR
深信服科技

核心业务系统安全接入



SANGFOR
深信服科技

将安全域最小化



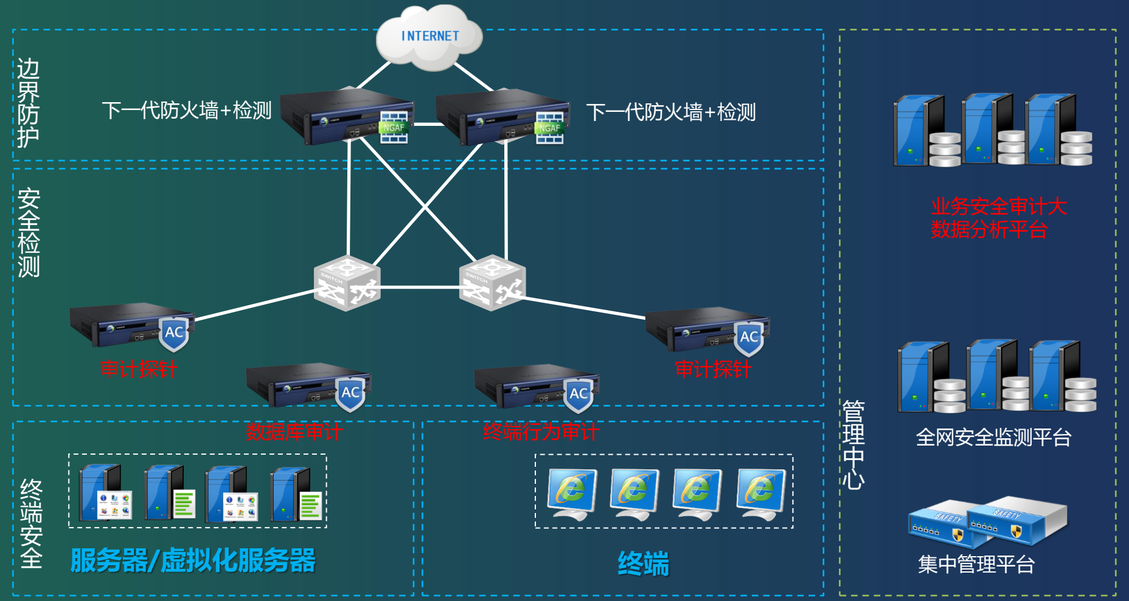
域安全

端点安全

SANGFOR
深信服科技

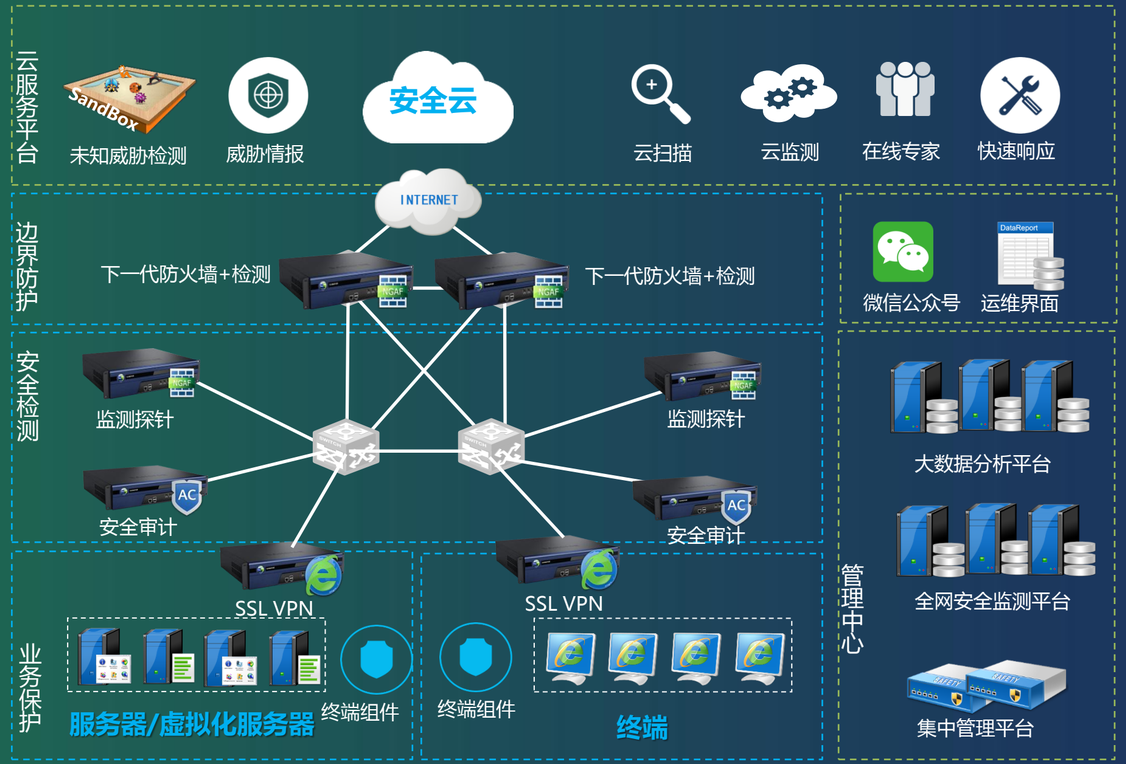
5、基于大数据的全局业务安全审计

- 用户-业务资产的访问行为审计
- 异常行为的黑客攻击追溯
- 多产品信息同步联动
- 支持数据库、认证系统、Web系统等数据中心应用



SANGFOR
深信服科技

数据中心安全建设
方案架构



SANGFOR
深信服科技

新技术的运用使数据中心安全边界模糊

云化

虚拟化

移动化