HUAWEI

华为云对公有云运维的思考

华为云安全运维负责人　邹继富

LEADING NEW ICT

目录

云服务面临的主要安全挑战

- 流量攻击，中断服务
- 账号窃取，获取权限
- 漏洞入侵，偷取数据

来自于外部的入侵攻击

- 共享环境下的隔离问题
- 如何保障数据的合法使用

云平台的内部风险

安全挑战

- 需要快捷、简单、易用、按需
- 需要统一管理
- 传统安全产品很难部署在云中

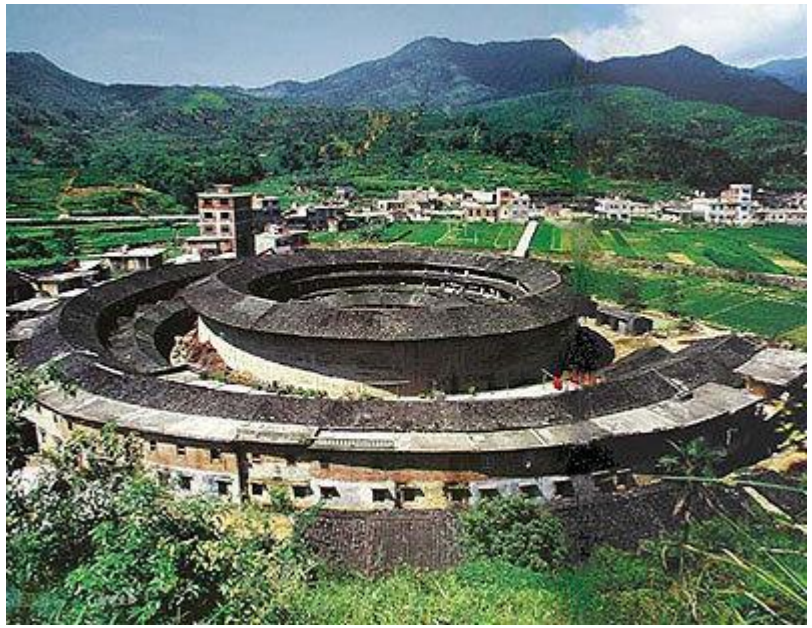
租户层的安全服务

- 租户数据防护不足
- 多数租户的安全意识有待提高
- 多数租户的安全技能有待提升

安全意识/技能待提高

公有云环境vs传统IT环境

传统IT环境-客家围楼



特点： 边界清晰，安全全责，业务可知
策略： 围墙式防护，安全可端对端覆盖，基于业务部署精细化防护策略
技术： APT攻击检测，钓鱼邮件防护，DLP

公有云-开放式小区

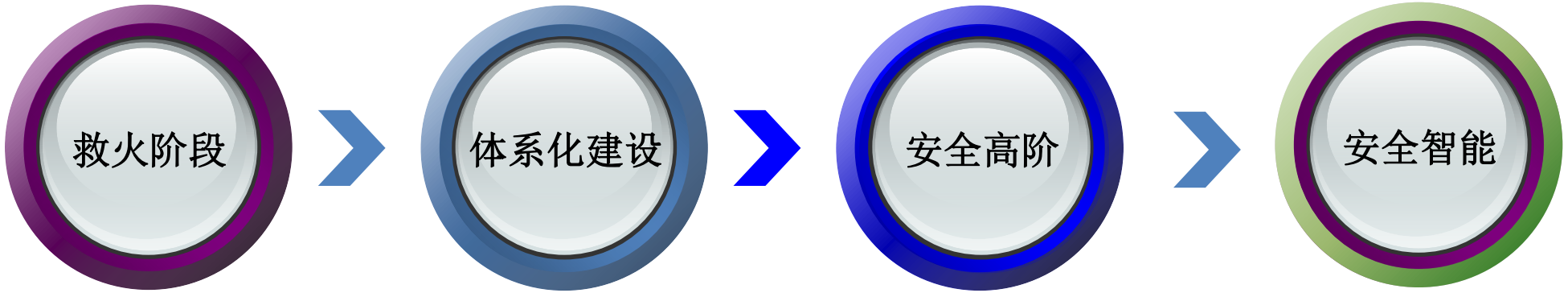
特点： 边界不清晰，安全责任共担，业务不可知
策略： 轻管控，重检测，快速响应，强调事后取证，
技术： 防DDoS攻击，防暴力破解及基于漏洞的攻击入侵，防云资源滥用等

公有云环境下的安全运维与传统环境下的安全运维的差异

类型	公有云安全运营	传统安全运营
防护环境	黑盒，业务不可知	白盒，业务可知
安全边界	责任共担，运维及网络边界模糊	边界清晰，端对端责任承担
安全目标	防攻击，防入侵，防滥用	防泄密，防攻击，防入侵
主要职责	检测，响应，安全咨询，安全服务，威胁建模开发等	监控，响应，配置安全策略
主要风险	拒绝服务攻击，弱密码及漏洞导致主机被入侵，云服务滥用	数据泄露，APT寄生虫，弱密码或漏洞导致入侵
安全产品	以自研产品为主，业务复杂，行业广，产品自身建模需要支持快速迭代，内容安全以违法违规检测为主	采用成熟的第三方解决方案和产品，安全能力受制于第三方产品的能力，内容安全采用DLP防止关键资产
技术手段	弱管控，注重检测，快速响应，控制防御通常采用黑灰名单机制，安全策略和业务平行运作，主要利用网络(DPI)进行数据挖掘和分析	强管控，控制防御通常采用黑白名单机制，业务及用户相对固定，一般通过业务属性制定安全策略，端到端可视，进行关联分析
典型技术	DDoS防御，暴力破解防御，WEB应用防护，内容检测，C&C通讯，网流分析可视	邮件安全，DLP，WEB应用防护，IPS, 移动端安全，主机安全

公有云安全运维挑战

华为云安全运维体系建设思路



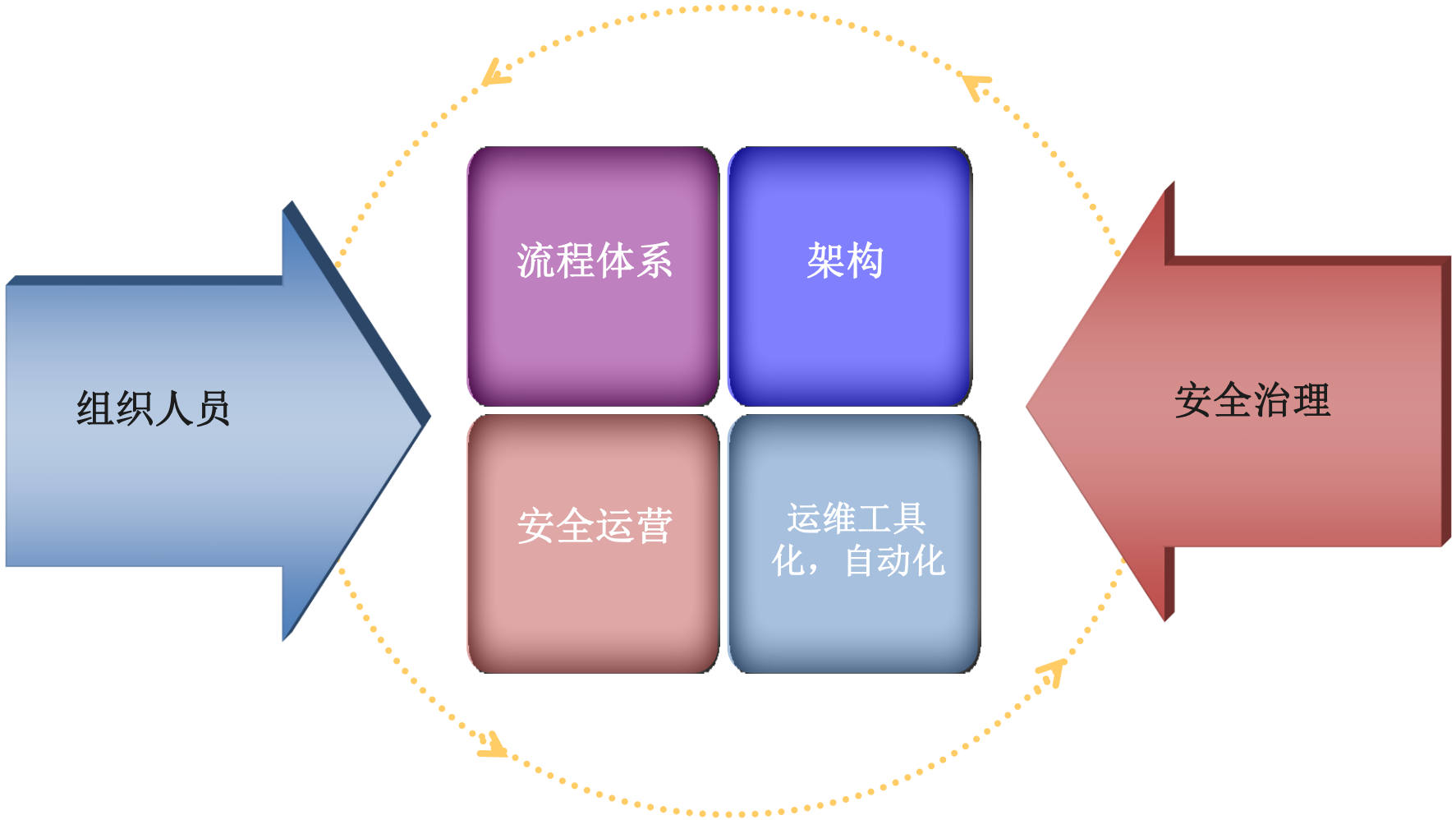
快速识别TOP风险，优先解决业务“痛点”，做一些基础的“保命”工作

扎实安全基础建设，建立安全运维流程体系+少量自研工具+第三方安全产品

自我研发和自动化
安全大数据
持续安全运维
关键能力矩阵布局

安全自适应，智能化，阻止，检测，响应，溯源，预测

华为云安全运维体系框架



安全运维流程体系

优秀实践、案例

AWS，Azure

法律+政策要求

国内立法机构
敏感国家立法机构

行业要求

行业政策、标准发布机构

执法要求、案例

国家监管执行机构
国家审查机构

历史案例

媒体事件、安全事件、运营事件

enisa European Network and Information Security Agency

CSA cloud security alliance SM

NIST National Institute of Standards and Technology U.S. Department of Commerce

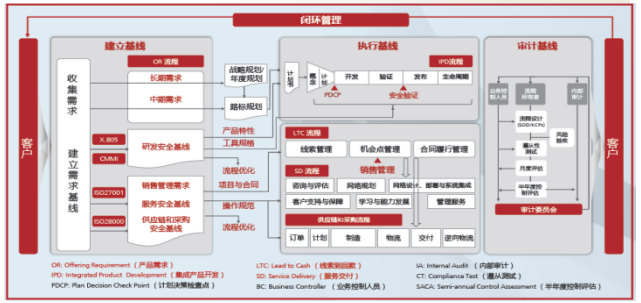
GDPR

中国网络安全等级保护

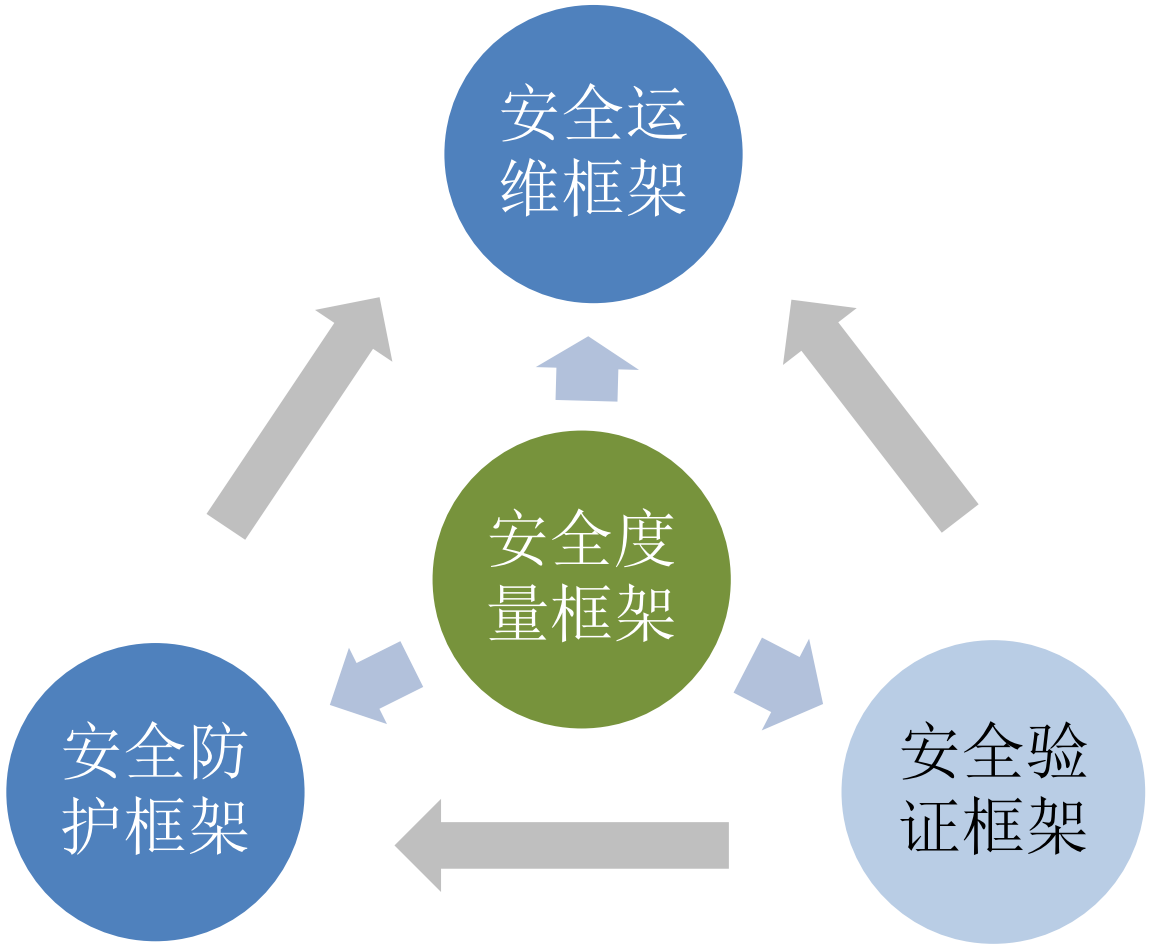
中共中央网络安全和信息化领导小组办公室
Office of the Central Leading Group for Cyberspace Affairs

满足行业客户的合规需求

满足云服务提供商内部端到端的管理需求



安全运维体系架构



✓**安全防护框架：**业务网络解耦，全旁路，可动态扩容，多层多维度感应头,包括入侵检测，DDOS防护，WEB应用防火墙，主机HIDS等

✓**安全运维框架：**负责信息日志收集和告警关联分析处理，基于大数据技术，对异常行为的实时安全监测，可实现态势感知，快速响应

✓**安全验证框架：**通过白盒及黑盒测试，对安全防护和运维框架进行检验，及时识别风险点和弱点，具体包括例行漏洞扫描，代码审计， 红蓝对抗

✓**安全度量框架：**衡量评价安全有效性, 包括检测有效性，事件响应时间，主动发现率，拦截响应时间，安全满意度等指标

安全运营

- 研发与运营团队深度合作
- 重点数据分析，威胁建模等关键能力人员培养
- 事件响应采用轮岗制
- 通过红蓝对抗演练及持续培训提高员工技能

人员

- 基于重大风险制定应急响应流程并定期演练
- 重点建立事前检测及响应流程
- 例行运营周报，月报通告机制

流程

- SDS,安全资源池化
- 以网络全可视化为核心能力，基于大数据分析能力，实现网络及业务威胁的快速检测能力
- 分散式取样，集中数据分析处理
- 常规应急响应自动化

技术

由基于边界安全的防护逐步发展为基于业务安全的防护

安全运维工具化，自动化

漏洞管理自动化

自动化黑IP识别及告警

分布式漏洞扫描系统

DDoS自动防御系统

自动化攻击预警及拦截

防火墙运维自动化

自动化攻击预警及拦截

Layer 2

基于特征对木马等恶意代码
注入或偷渡进行检测和告警

Layer 4

态势感知，基于信誉等级进行
智能学习并对异常进行告警

Layer1

对常规扫描，暴力破解等攻击
进行实时告警并阻断拦截

Layer 3

基于行为进行异常检测，对常规CC通
讯，对外攻击，扫描进告警并拦截.

Layer 5

采集取证攻击相关攻击日志和
告警信息，可作为反制的手段

Anti-DDoS

秒级IP封堵

与运营商联动，实现对被攻击IP自动拉黑洞，秒级生效，快速释放被攻击带宽

DDoS攻击可视

针对流量、会话型洪水攻击在云边界进行手术刀式清洗，提供高达5G的防护能力攻击超阀值实时告警，显示流量情况

云端防护

通过智能调度系统，利用高防机房大带宽，实现对业务提供高达300G的4到7层的抗D能力，应对超大流量攻击，保障业务连续性

业务上云安全“12字真言”，消除90%以上的外部攻击风险

强口令

修改所有OS系统口令（包括管理员和普通用户）、数据库账号口令、应用（WEB）系统管理账号口令为强口令，密码12位以上。

关端口

禁止不必要的端口直接暴露在公网。设置防火墙规则或配置安全组策略来禁止端口开放情况，推荐使用安全组策略。非公共开放的业务端口（如SSH），建议设置只允许特定的IP进行连接。

控权限

严格控制各服务的系统权限，各服务进程请不要以root权限运行；各应用(如WEB)同数据库交互的账号同样不要使用root权限的账号。

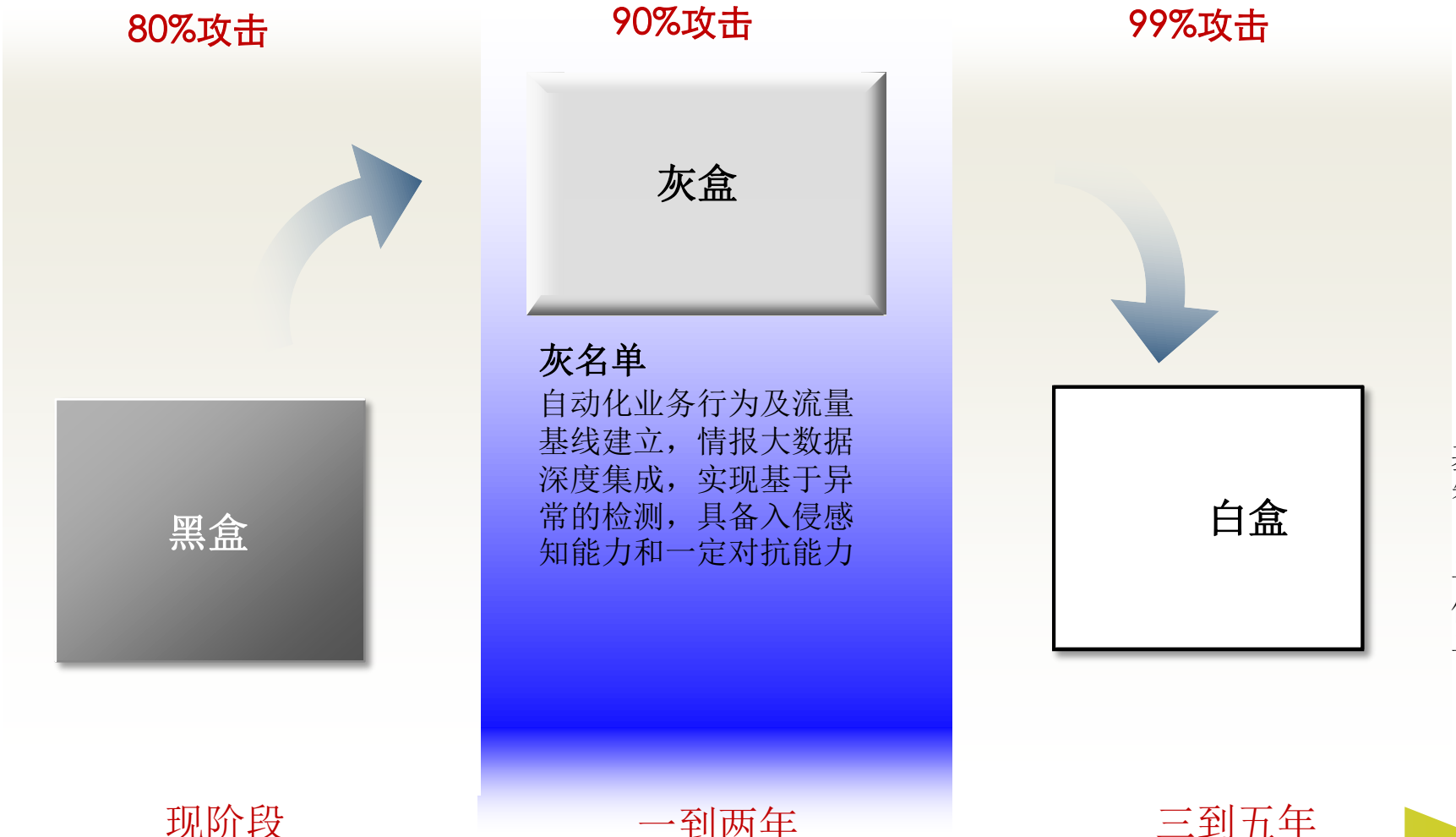
查应用

检查WEB应用及相关配置是否存在安全风险（如SQL注入、XSS、struts2框架等漏洞；各项配置是否安全等）

对未来云安全的一点思考

黑名单

实现网络全量可视；基于特征检测；人工灵活建模；事件驱动持续优化，快速迭代；响应采用灰度处理机制；由被动到主动防御;



白名单

基于大数据，人工智能的安全检测，自适应，动态白名单机制，通过基于信誉度的多级白名单进行控制。

THANK YOU