



全面智能化安全服务中心的 建设思路与实践

演讲人：北京安数云信息技术有限公司 吴雷

目录

CONTENTS

01. 现状

02. 解决方案

03. 应用场景

04. 优势

01.现状:合规

国家标准、行业标准、国际标准



<<信息安全技术网络安全等级保护基本要求>>

<<信息安全技术云计算服务安全能力要求>>

<<政务云安全要求>>

<<云计算安全技术要求 第2部分: IaaS安全技术要求>>

01.现状

1、安全策略配置复杂

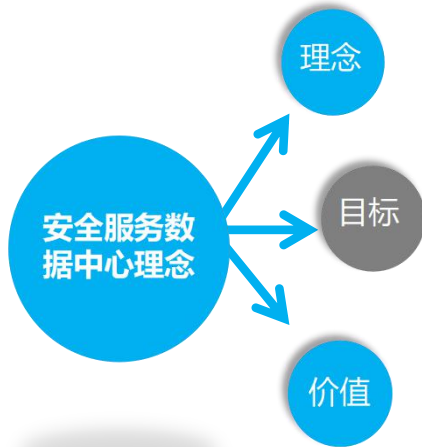
2、运维复杂

3、数据浪费

4、安全的集中管控



02.解决方案



中心理念

“安全服务数据中心”：安全服务标准化能力、安全服务多样化能力、威胁识别能力、自动编排能力、动态弹性伸缩能力等

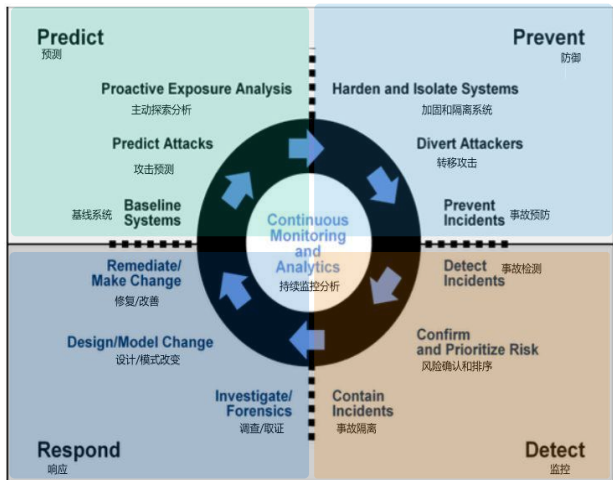
中心目标

通过 **“软件定义安全 (SDS)、软件定义网络 (SDN)、NFV、大数据”** 等核心技术 建立起动态的、闭环的软件定义的云安全服务体系

中心价值

简单 敏捷 合规

02.解决方案



等保合规

- 安全边界区域
- 安全技术环境
- 安全通讯网络
- 安全管理中心



智能化

- 智能化编排
- 动态防御策略
- 安全自动防御



安全既服务

- 租户安全服务
- 构建安全服务
- 分布式架构



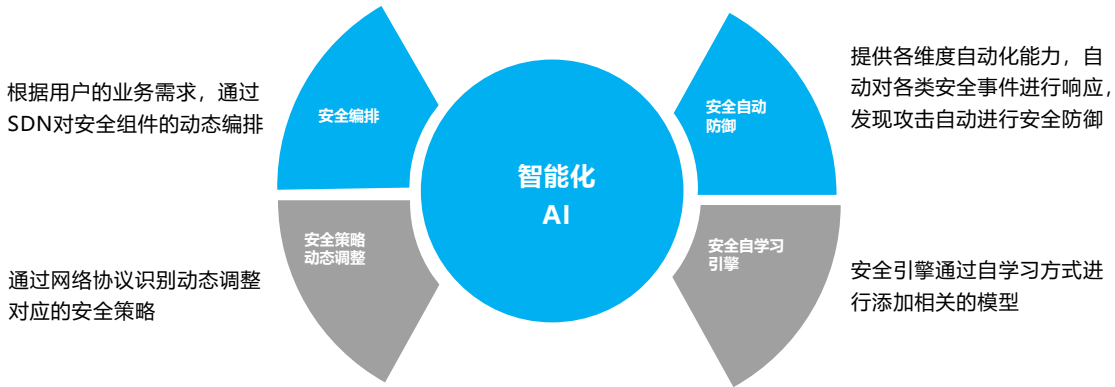
全程可视

- 资产可视化
- 防护可视化
- 数据流转可视化

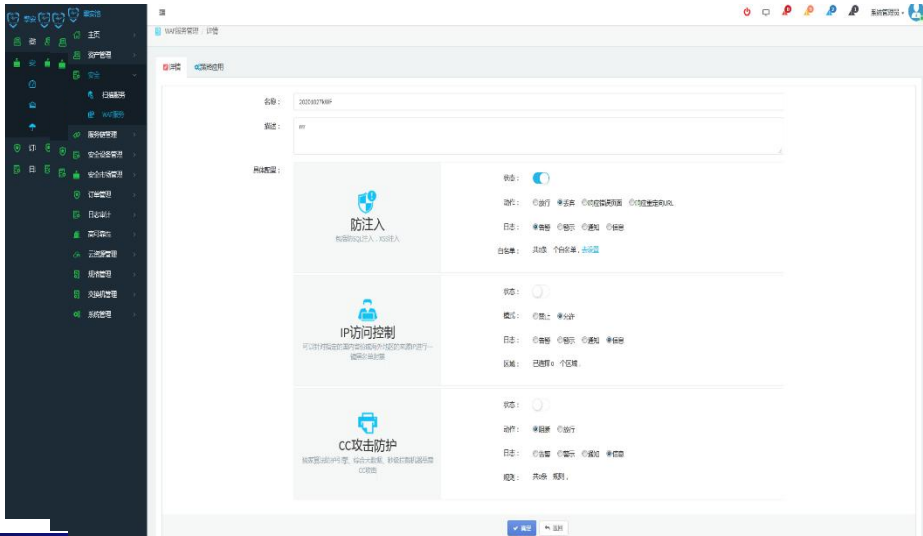
02.解决方案：等保合规



02、解决方案：安全动态编排



02.解决方案：安全即服务



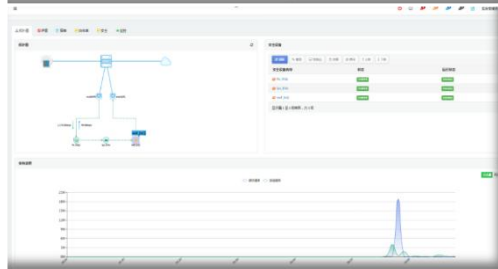
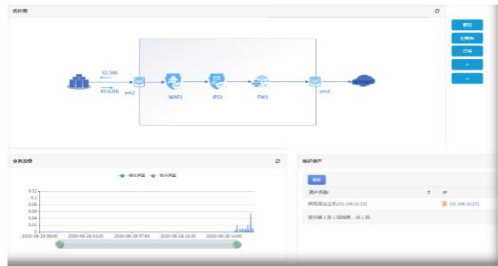
1. **方便：**用户直接使用，帮助大部分用户简单、方便使用

2. **灵活：**管理员可以在后台随意编辑各种安全服务组合，方便用户使用

3. **可靠性：**所有的后台安全实例全部是分布式架构

4. **成本：**一个安全实例可以给多个用户共用，可以有效的降低用户使用成本

02.解决方案：可视化



02.解决方案：可视化

资产态势

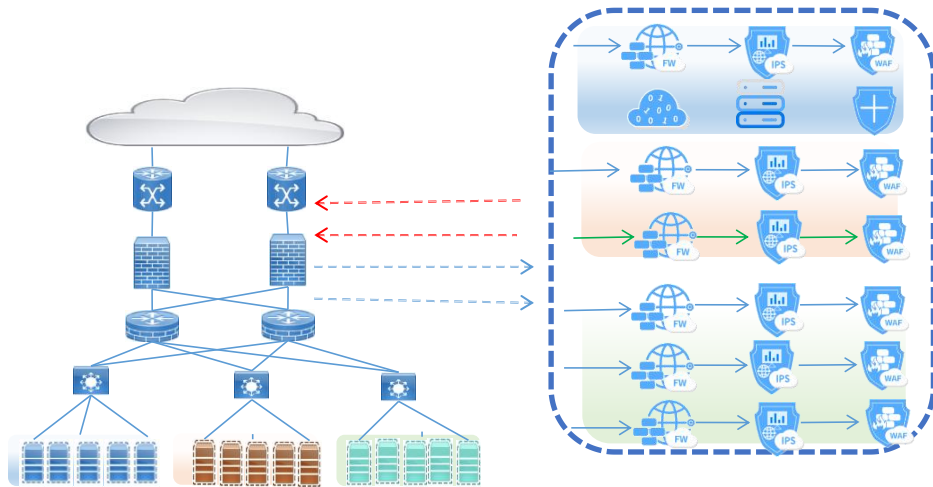
攻击态势

用户画像

追踪溯源

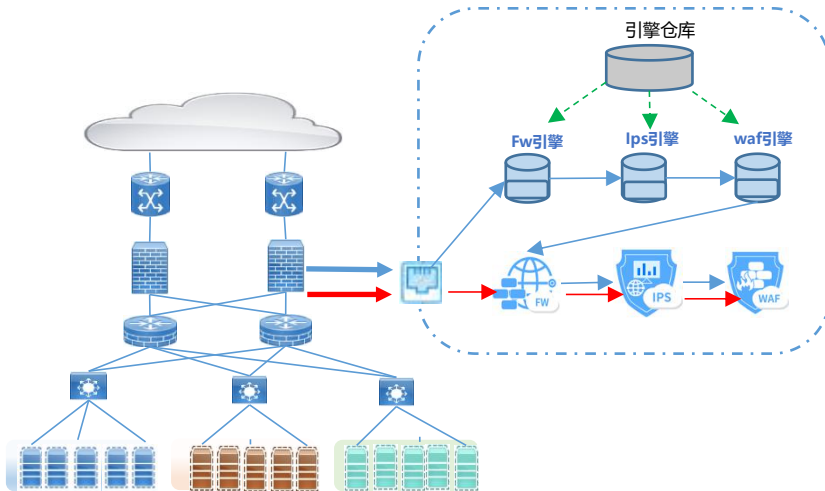


03.应用场景：安全动态编排



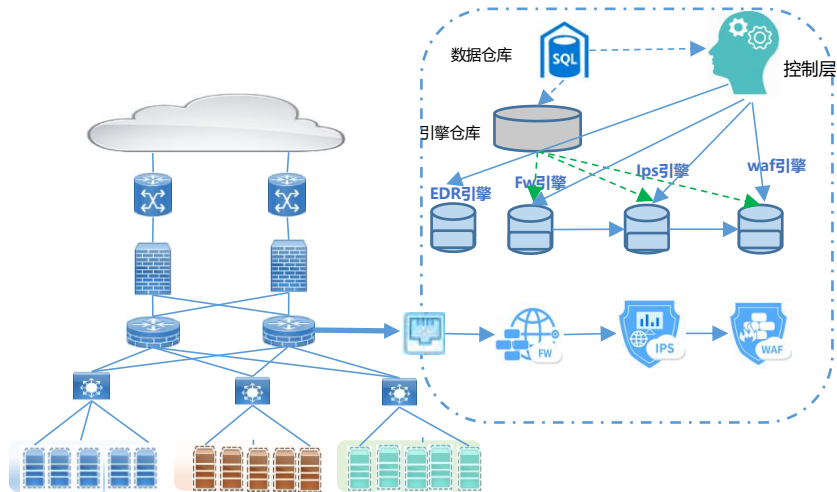
1. **业务1**：等保2级要求，自动安全服务编排
2. **业务2**：等保3级要求，自动安全服务编排（主备）
3. **业务3**：负载均衡能力，会随着业务动态的扩展安全资源及安全服务链
4. **智能化waf**：自动识别网站流量，网站流量经过waf清洗，非网络流量绕过去
5. **可靠性**：软bypass，及服务链的切换

03.应用场景：策略动态调整



1. **第一个业务报文：** 上送对应的安全引擎，经过每个引擎分析，下发对应的安全策略给下面的安全实例
2. **后业务报文：** 不需要在上送安全引擎，直接走对应的安全服务链
3. **业务迁移后：** 没有对应的业务经过对应的服务链删除之前下发的安全策略

03.应用场景：策略动态调整



1. **大数据分析：**通过大数据分析识别安全威胁，通知控制层
2. **控制层：**通过确认，一键式下发安全策略,联动多个安全能力
3. **安全设备：**安全设备接收下发的安全策略，达到整体安全效果

04.优势



兼容第三方安全

安数云的平台兼容第三方的虚拟安全设备，用户可以根据自己的需求采购第三方的虚拟安全设备，放在资源池中统一管理。



可靠性

虚拟化安全设备故障、硬件设备故障都不影响用户业务，都是秒级切换M:N机制。



性能

单租户的流量不在局限在单独虚拟机，通过核心的技术把单租户流量横向扩展到10G流量，并且兼容第三方的虚拟安全设备。



编排硬件安全设备

可以不在采购硬件SDN交换机的基础上，把传统硬件和虚拟化安全进行统一的安全服务链编排，同时赋能SAAS服务给传统硬件。



图形化编排

完全通过图形化进行服务链的编排操作，简单方便。

04.优势



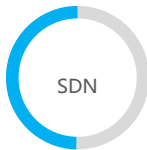
智能化

安数云为客户自动化的安全服务套餐，服务链，相关的安全策略下发，安全能力的联动。最大程度的减少管理员的运维压力。



安全合规

安数云为客户提供了等级保护所需要的各类安全服务,为租户供等级保护差距分析能力、安全整改和安全运维等服务，实现客户网络安全工作的合规。



SDN

安全云的底层智能化的基础能力之一是基于SDN实现的，通过SDN可以更加灵活的编排安全服务及应用到可靠性、性能、智能化等方面。是下一代安全的框架核心技术之一。



SAAS安全服务

安数云提供SaaS的安全服务，可以给不同的租户更灵活的安全服务，使用户使用起来更加灵活、方便。



安全设备共享

安数云提供的虚拟安全设备可以给30-50个租户共用，更大程度上帮助用户减少采购成本，同时满足租户的隔离等保等要求。



THANKS