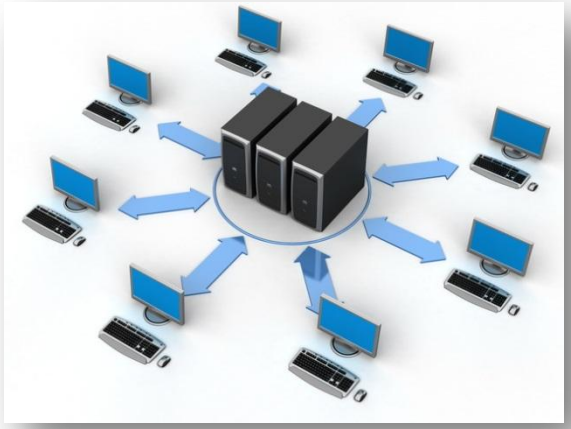
智能防火墙在高校行业中的应用

政府行业技术总监 杜旭晖

2014/04

高校行业已成为山石重点行业之一



CERNET地区主节点高校中的7所高校、省级节点高校中的14所高校选Hillstone

150+高校，47所211工程院校、17所985高校选择Hillstone

17+高校选择Hillstone数据中心防火墙，支持大流量大并发互联网访问

14所Cernet地区及省高校节点选择山石

提纲

1 山石下一代智能防火墙的理念和价值

2 山石下一代智能防火墙在高校的应用

智能和虚拟化是山石的两大主力技术方向

安全技术发展

未知威胁（APT/0-day）

威胁 -> 风险

被动 -> 主动

智能下一代防火墙（iNGFW）

网络技术发展

虚拟化数据中心

SDN/NFV

虚拟弹性架构

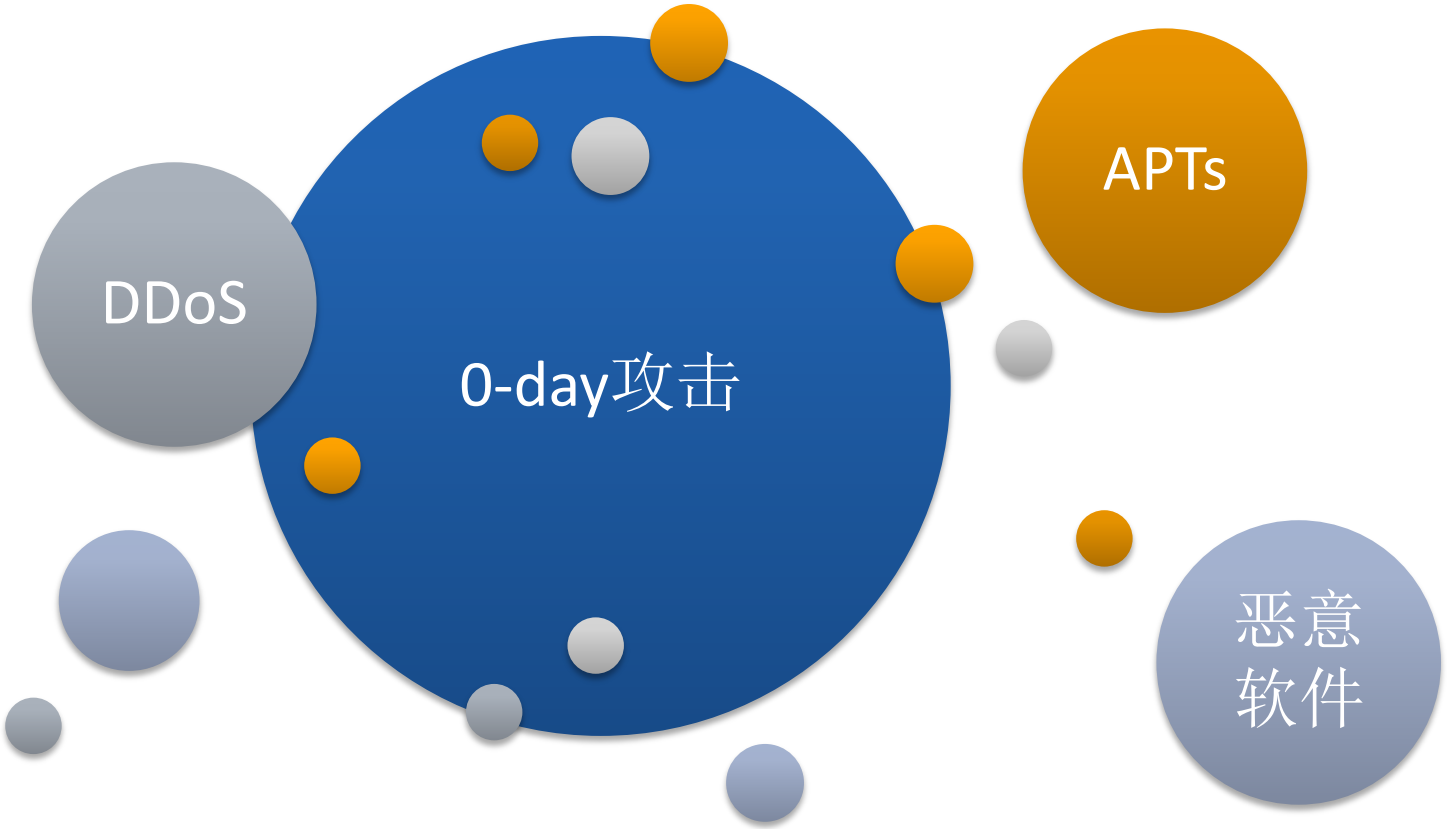
智能安全成为趋势


THE NEXT LEAP FORWARD FOR THE FIREWALL
LAYER 7
Next Gen Firewall
Intelligent Firewall
STATIC
DYNAMIC
Traditional Firewall
LAYER 3

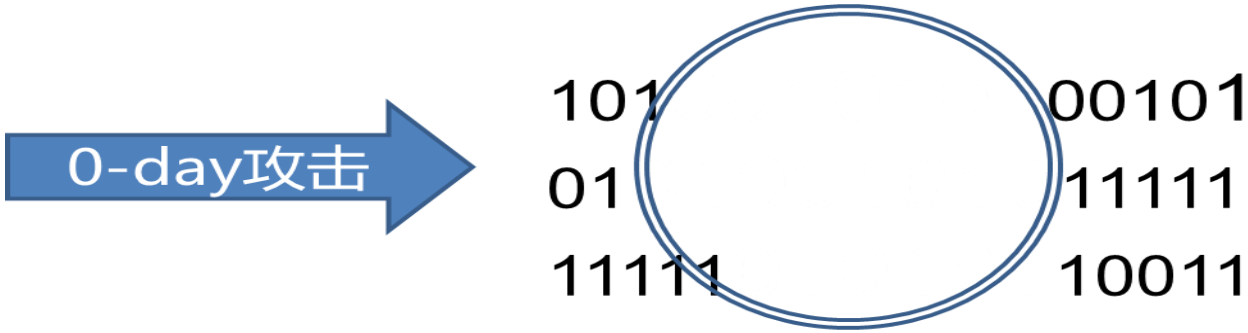

SMART SECURITY
doesn't back you into a corner.
Get access to the industry's
Best-Of-Breed Technologies

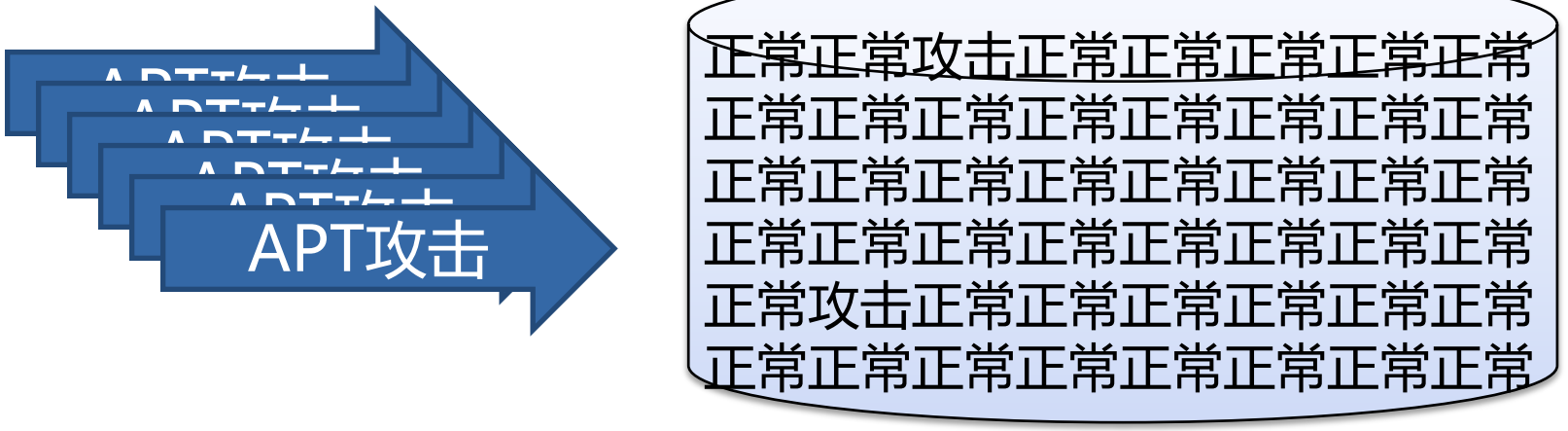

Intelligent Cybersecurity for the Real World

0day攻击依然是当前无法根本解决的问题

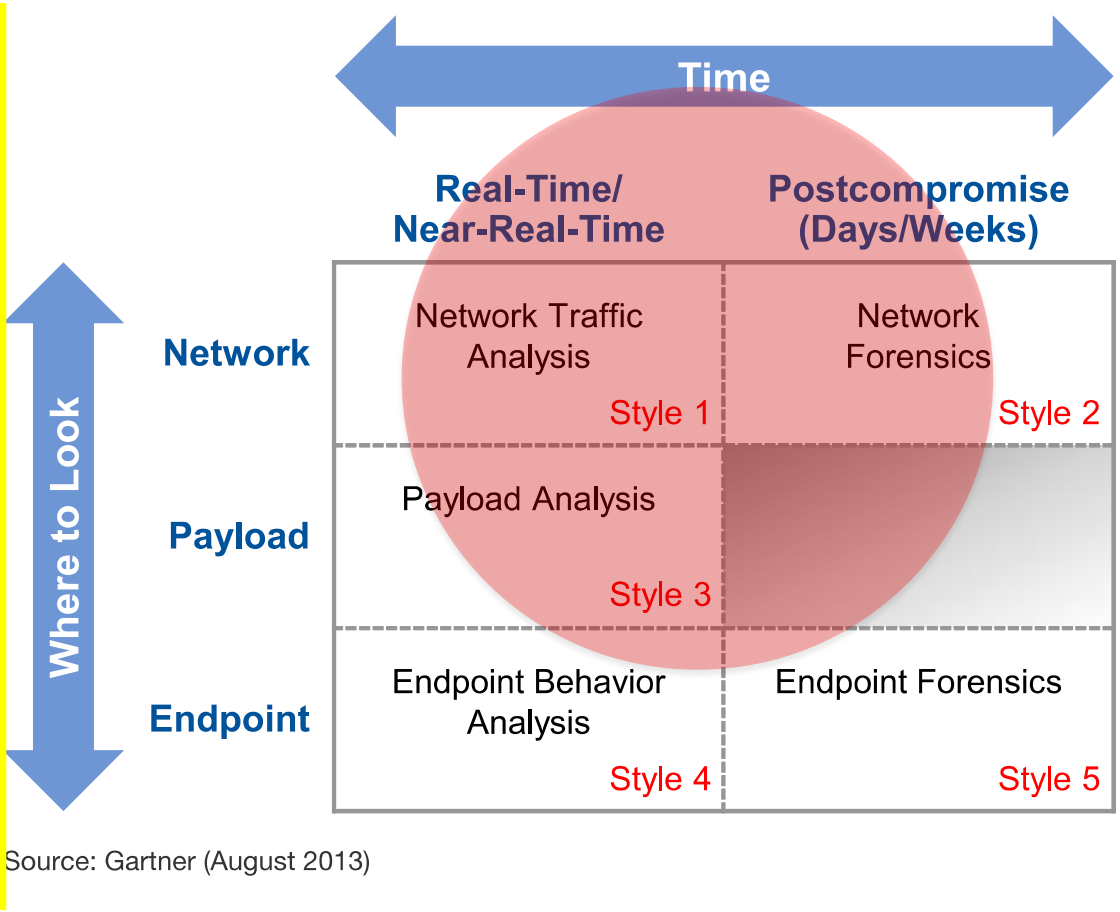


根本在于目前的检测以“特征”为核心





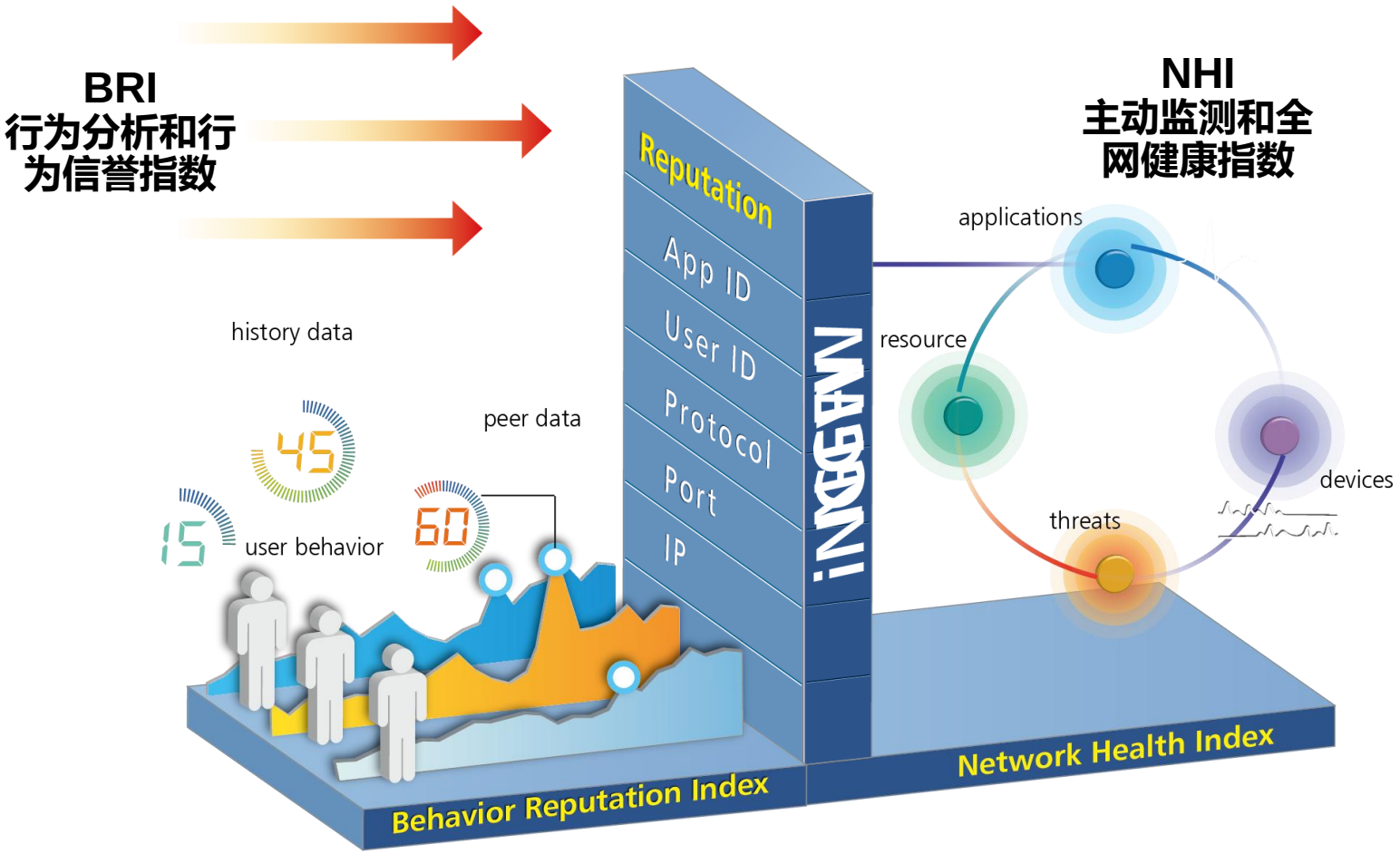
Gartner给出的解决方案



Source: Gartner (August 2013)

攻击发现 + 攻陷后发现 + 事件反应

下一代智能防火墙就是在网络和行为两个维度的延伸



Intelligent NGFW

网络健康指数NHI

网络连通

0-100

80分

设备资源

0-100

50分

30分

业务服务

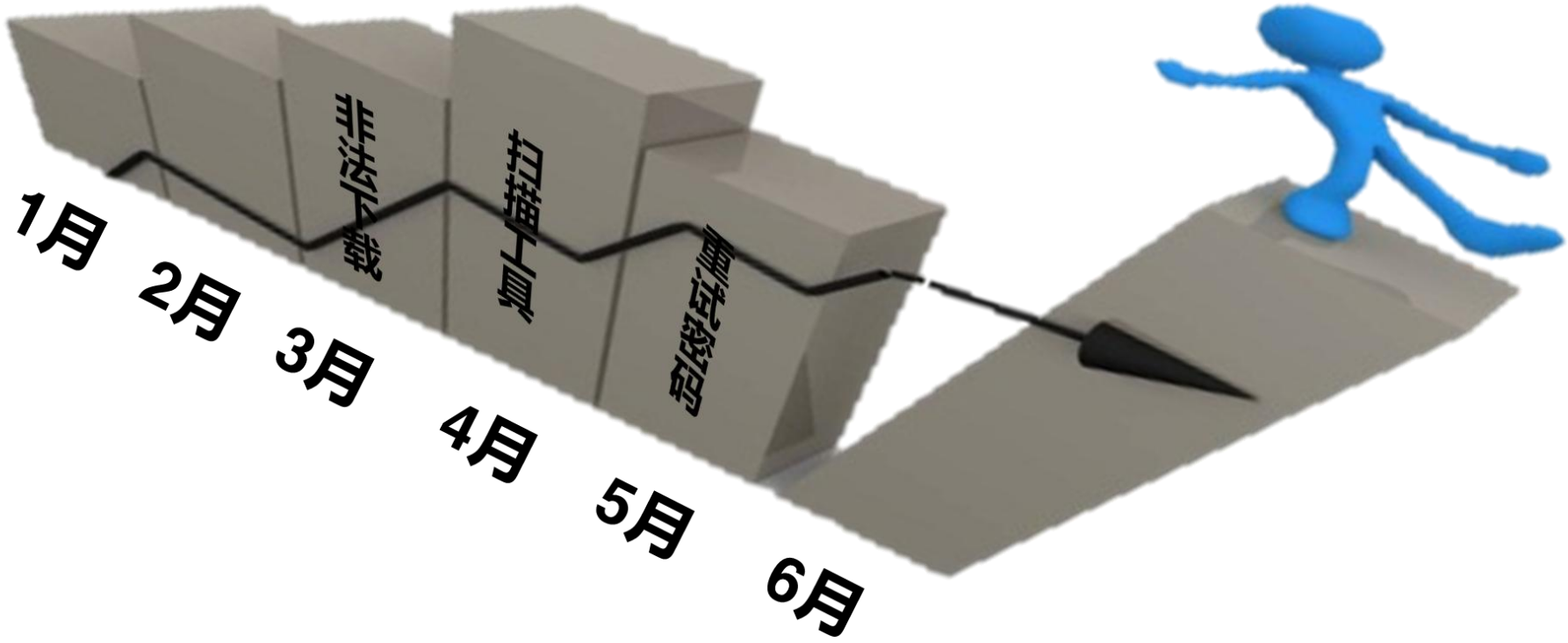
0-100

30分

全网健康指数NHI

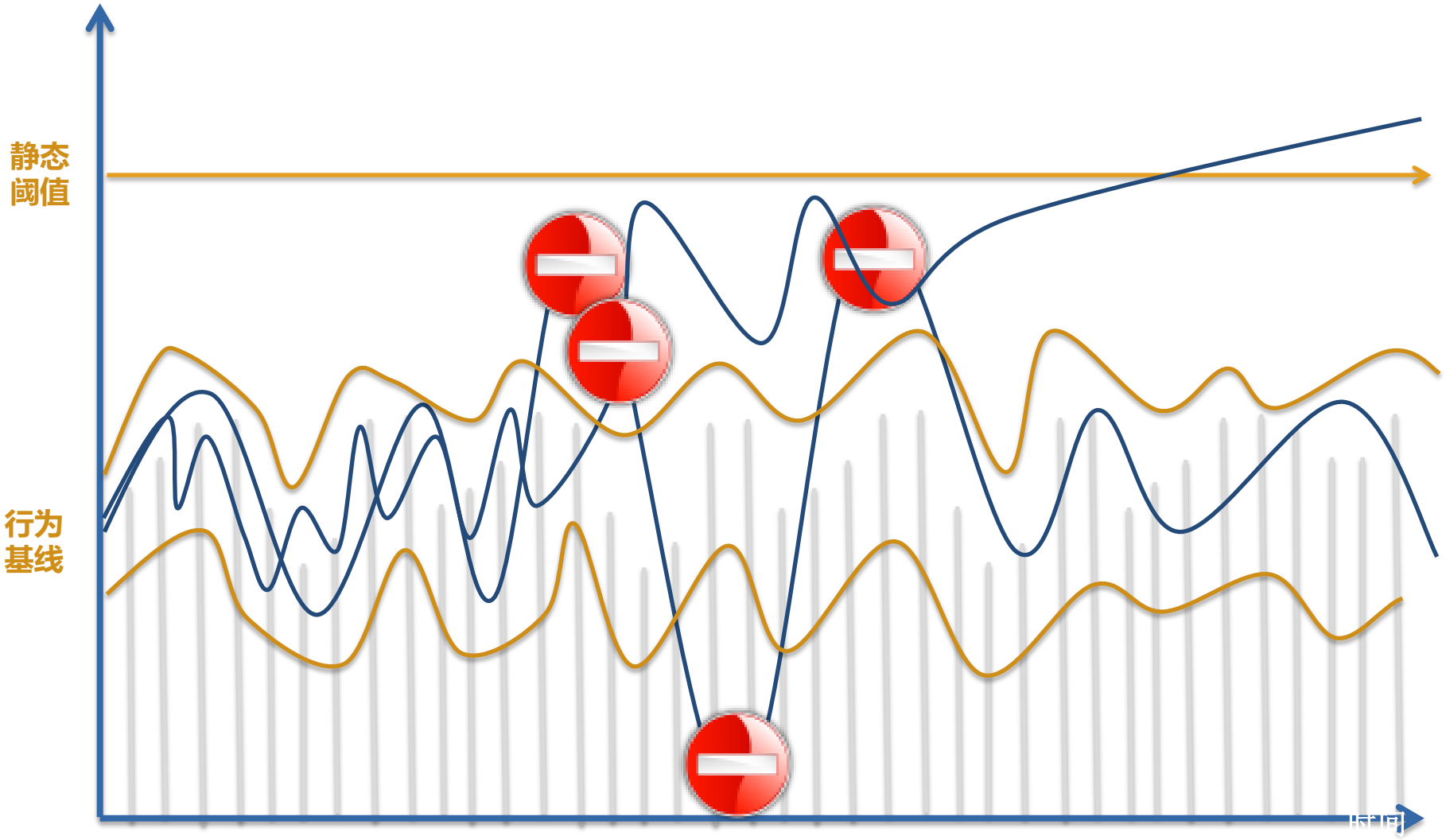
设备资源检测	网络节点检测	业务服务节点检测
• CPU使用率 • 内存使用率 • 新建连接速率 • 并发连接数 • SNAT端口使用率 • 接口流量 • 磁盘使用率 • 机箱温度 • CPU温度	对与设备相连的三层交换、路由器等网络节点的可达性和可用性实时探测	对网络里Web、邮件、文件服务（FTP）、LDAP、DNS等关键业务的可用性实时探测

行为信誉指数BRI



50分 行为信誉指数

关键技术：行为基线和特征分析

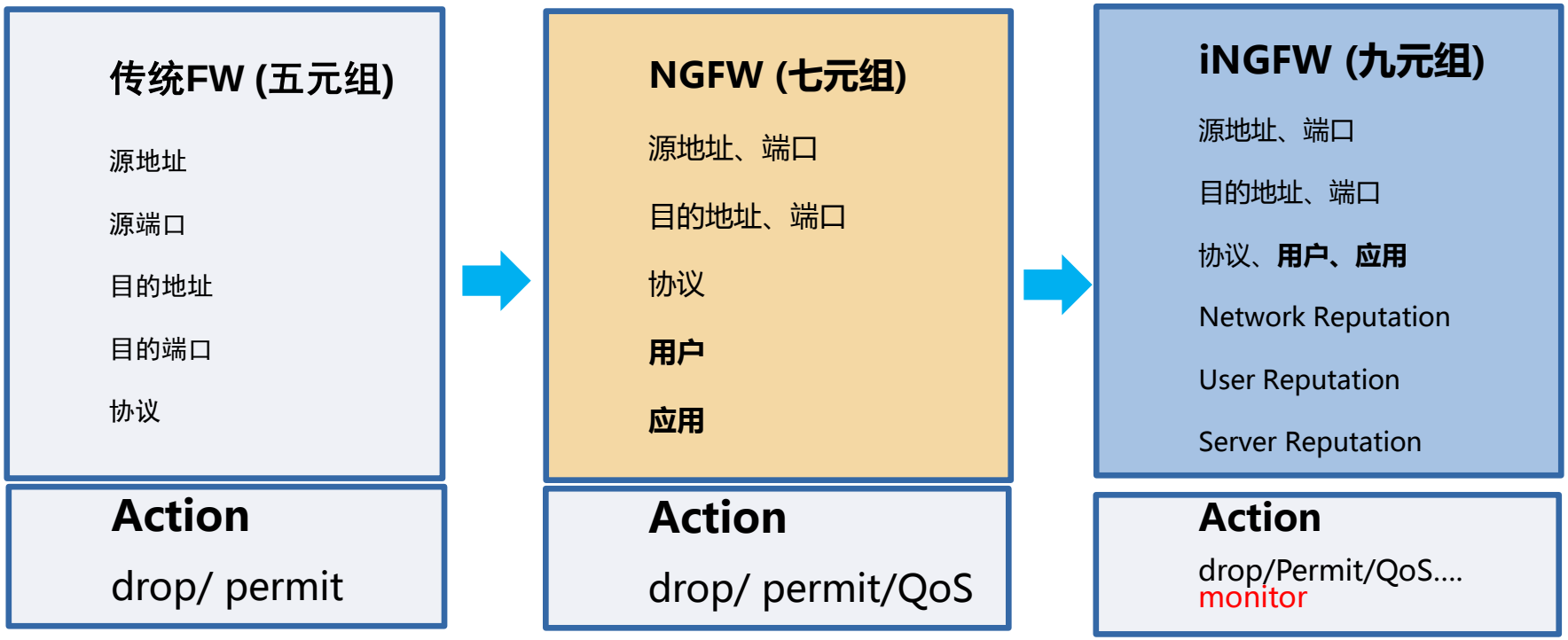


通过动态行为基线和行为特征来更早更准发现异常

基于用户和服务的风险

对象	风险域	风险项	说明
user	静态属性	USER ID	user唯一属性
		终端节点	包含IP、mac、硬件信息等
		终端类型	PC/mobile/PAD
		接入接口	未来可考虑增加接口风险评估
		安全域	未来可考虑增加安全域风险评估
		所属组	user group
	应用属性	app	user的top N app
	威胁属性	恶意软件下载防护	下载或传播病毒、木马、蠕虫等等
		应用层攻击	user发起的攻击
		攻击防护	user发起的攻击
		botnet防护	botnet检测，包含特征方式和数据挖掘方式
		未知威胁	已user为对象的异常行为分析结果
	合规属性	数据泄露	user外发敏感数据
		URL	访问非法网站、钓鱼网站等高风险级别，游戏、娱乐等为低风险级别
		网络私接	无线私接、NAT私接等等
		policy deny	非法行为动作认为存在风险
server	静态属性	服务器类型	例如是web还是mail，Apache是哪个版本，不同的版本存在的漏洞以及被攻击手段是不同的。
		接入接口	未来可考虑增加接口风险评估
		安全域	未来可考虑增加安全域风险评估
	应用属性	APP	对于服务器只需要存在提供服务的应用和管理需要的应用(telnet，ssh等)，其他无关的应用存在风险
	威胁属性	木马	木马攻击
		web攻击	针对性web服务器攻击
		应用层攻击	被应用层攻击
		网络攻击防护	被网络层攻击
		botnet	包含特征方式和数据挖掘方式
		未知威胁	已server为对象的异常行为分析结果
	可用属性	流量	流量基线分析
		连接数	连接数基线分析
		网络延迟	网络延迟基线分析
		丢包率	丢包率主动检测

基于信誉的闭环智能控制



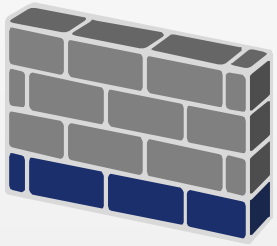
问题

- 同一用户，无论Reputation如何变化，其访问权限是静态不变的。
- 同一Service，无论Risk如何变化，其所加载的安全策略也是静态不变的。

After

- 同一用户，信誉变化后，其访问权限也随之**动态**变化。
- 同一Service， 风险变化后，其加载的安全策略也随之**动态**变化。

智能让安全更主动

单纯的执行者	建议者	**建设性的执行者**
		
防火墙	智能安全分析	**下一代智能防火墙**

提纲

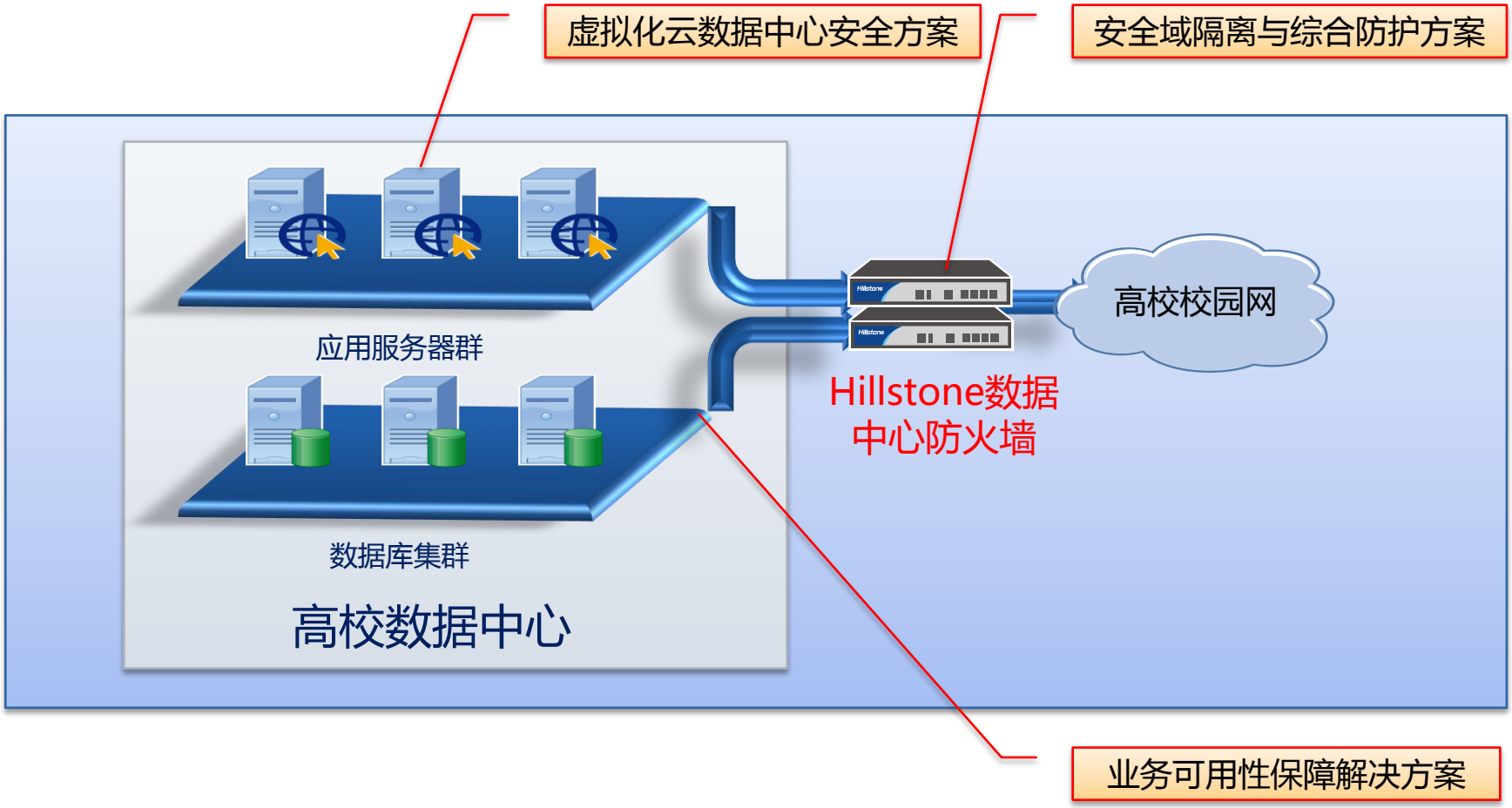
1. 山石下一代智能防火墙的理念和价值

2. 山石下一代智能防火墙在高校的应用

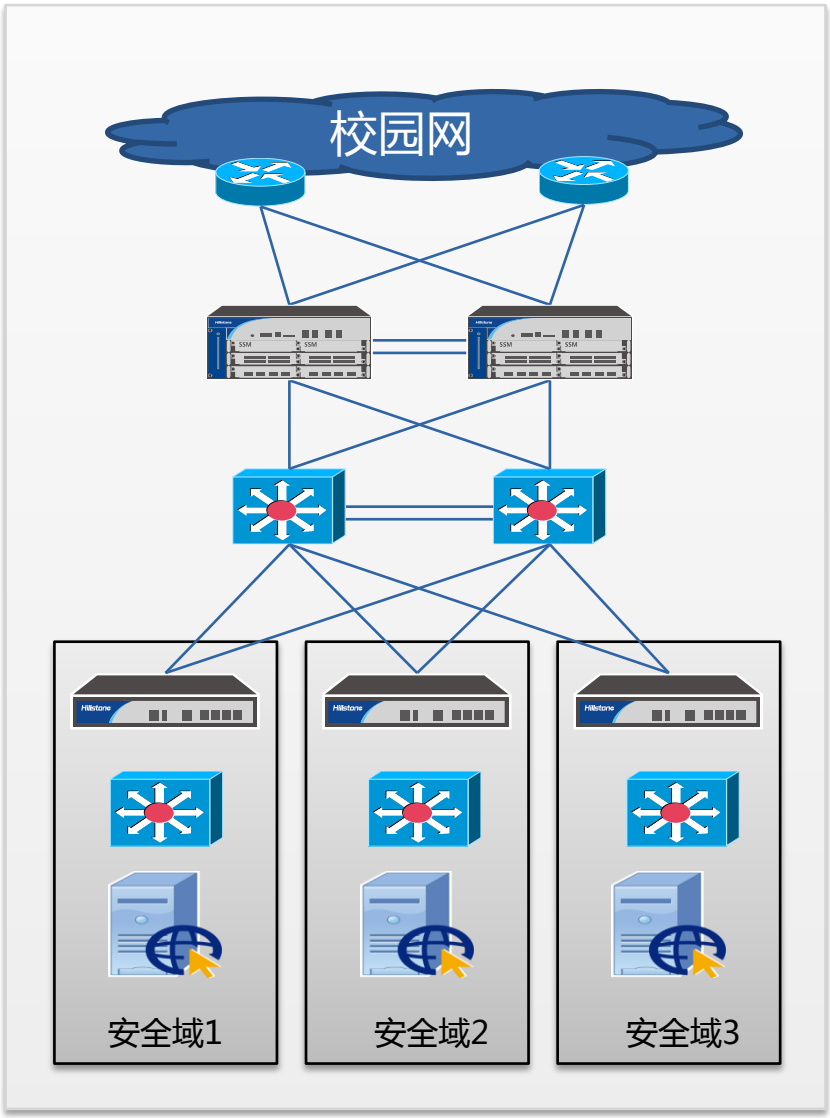
高校用户的典型应用场景

高校互联网出口	高校数据中心智能防护
业务特点： ✓ 多运营商、多链路 ✓ 大并发、海量访问 ✓ Cernet2覆盖大部分211高校（IPv6） 安全需求： ✓ 高性能NAT及上网访问控制 ✓ 流量管理（基于应用的流量管理） ✓ 多链路负载均衡 ✓ 计费&实名制审计 ✓ 双栈支持（IPv4 & IPv6）	业务特点： ✓ 大量计算资源集中 ✓ 大并发访问 ✓ 部分院校引入了虚拟化技术 安全需求： ✓ 对抗渗透性攻击 ✓ 网络可用性保障 ✓ 持续性攻击防护 ✓ 可支持虚拟化计算环境

山石高校数据中心安全接入方案



山石安全域隔离与综合防护方案



多种部署方式

- 透明接入、路由接入、全交叉冗余接入、旁挂接入、单臂接入

多种安全功能

- 防火墙访问控制、入侵防御、病毒过滤、Qos、抗攻击
- 按需开启防护功能

多种路由协议

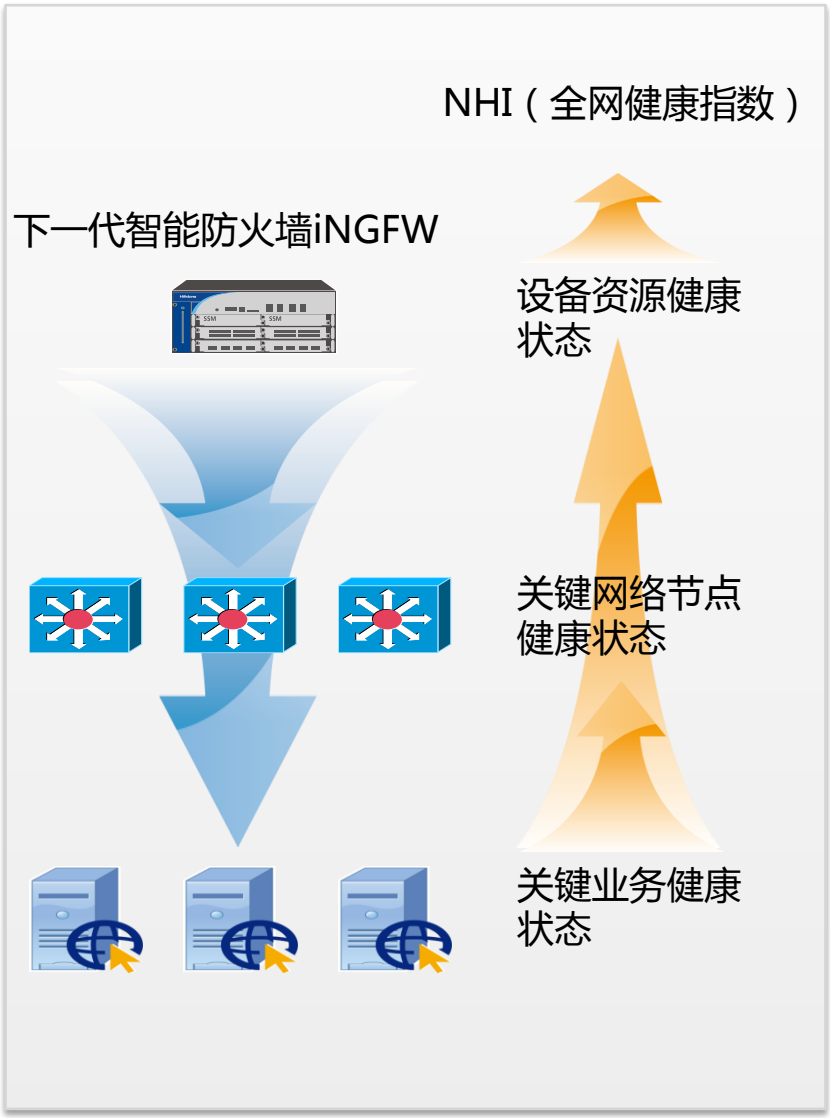
- 静态路由、动态路由、策略路由、基于应用的路由

接入认证与控制

- 多种认证技术：本地认证、Radius、AD、LDAP

集中安全审计

山石业务可用性保障解决方案



主动检测

- 设备资源健康状态检测
- 关键网络节点健康状态检测
- 关键业务服务健康状态检测
- 汇总形成量化的全网健康指数（NHI）

安全预警

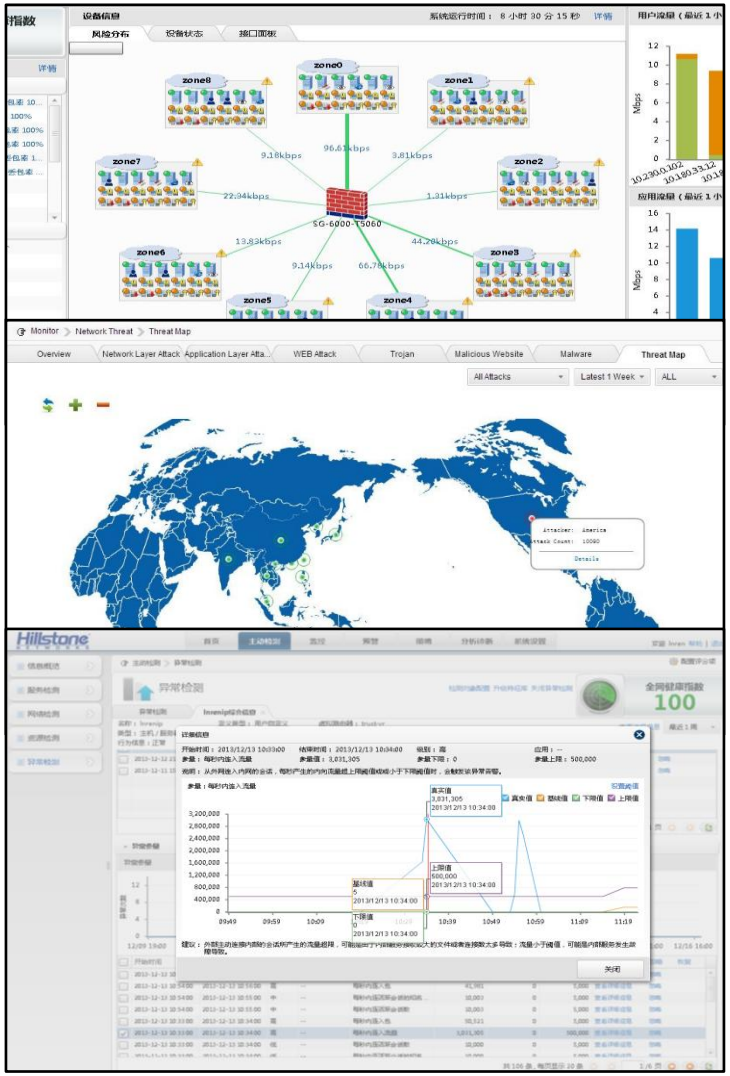
- 安全健康状态变化
- 业务流量的异常变化
- 并发连接的异常变化

安全监控

- 设备监控：设备资源状态
- 用户监控：流量和并发状态
- 应用监控：应用流量和并发状态
- 管道监控：Qos管道状态监控
- 服务网络监控

全网健康报告

山石行为信誉分析解决方案



行为基线管理

- 动态学习对象的流量基线，根据基线分析得到的结果；
- 按周期学习对象的20种参量模型；

行为异常分析

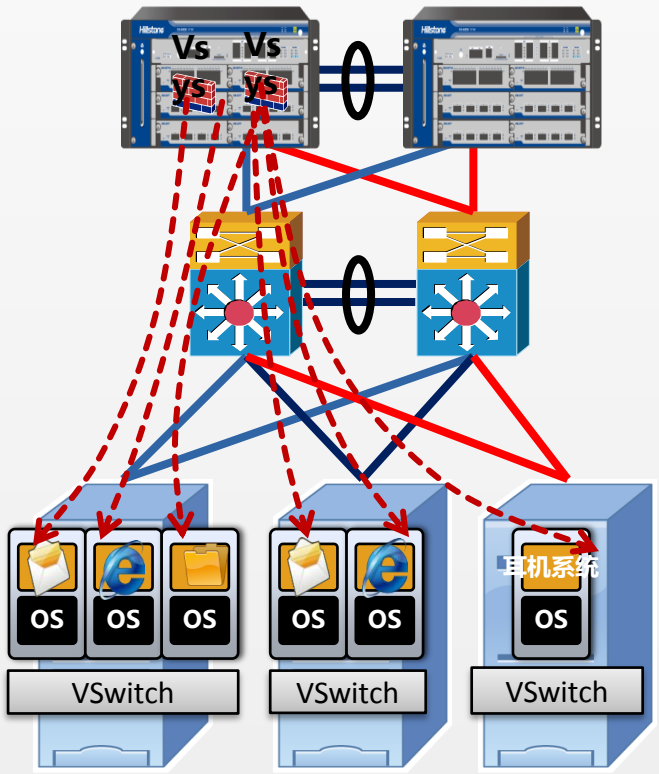
- 所有配置的对象进行实时监控检测
- 与自学习的对象基线进行对比
- 超过基线的信誉评分管理

未知威胁分析

- 多种异常行为的关联分析
- 根据异常行为匹配威胁特征
- 与全网健康指数的关联分析
- 威胁来源可视化分析

行为信誉后的动态规则响应

山石虚拟化环境中的隔离与控制方案



隔离南北向流量

- 传统数据中心边界隔离与安全防护方案

流量牵引东西向流量隔离

- 虚拟化环境下不同虚拟机间流量的隔离与安全防护

虚拟防火墙

- 为不同的虚拟机提供独立的安全控制平面
- 不同虚拟防火墙资源独立配置，策略独立管理
- 不同虚拟防火墙也面向不同的接入访问用户提供差异化的安全管控

旁挂式部署支持

- 减少对网络配置的改造难度

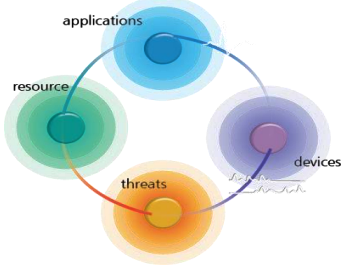
案例1：在某高校IDC的应用

同时要管理100+服务器

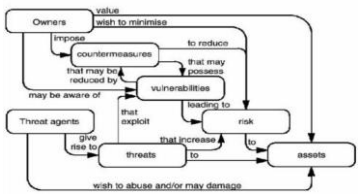
经常发生网络畅通，但业务访问过慢，并发投诉

希望能够在业务服务变慢的过程中能够提早发觉并提前响应

能够迅速直观地定位



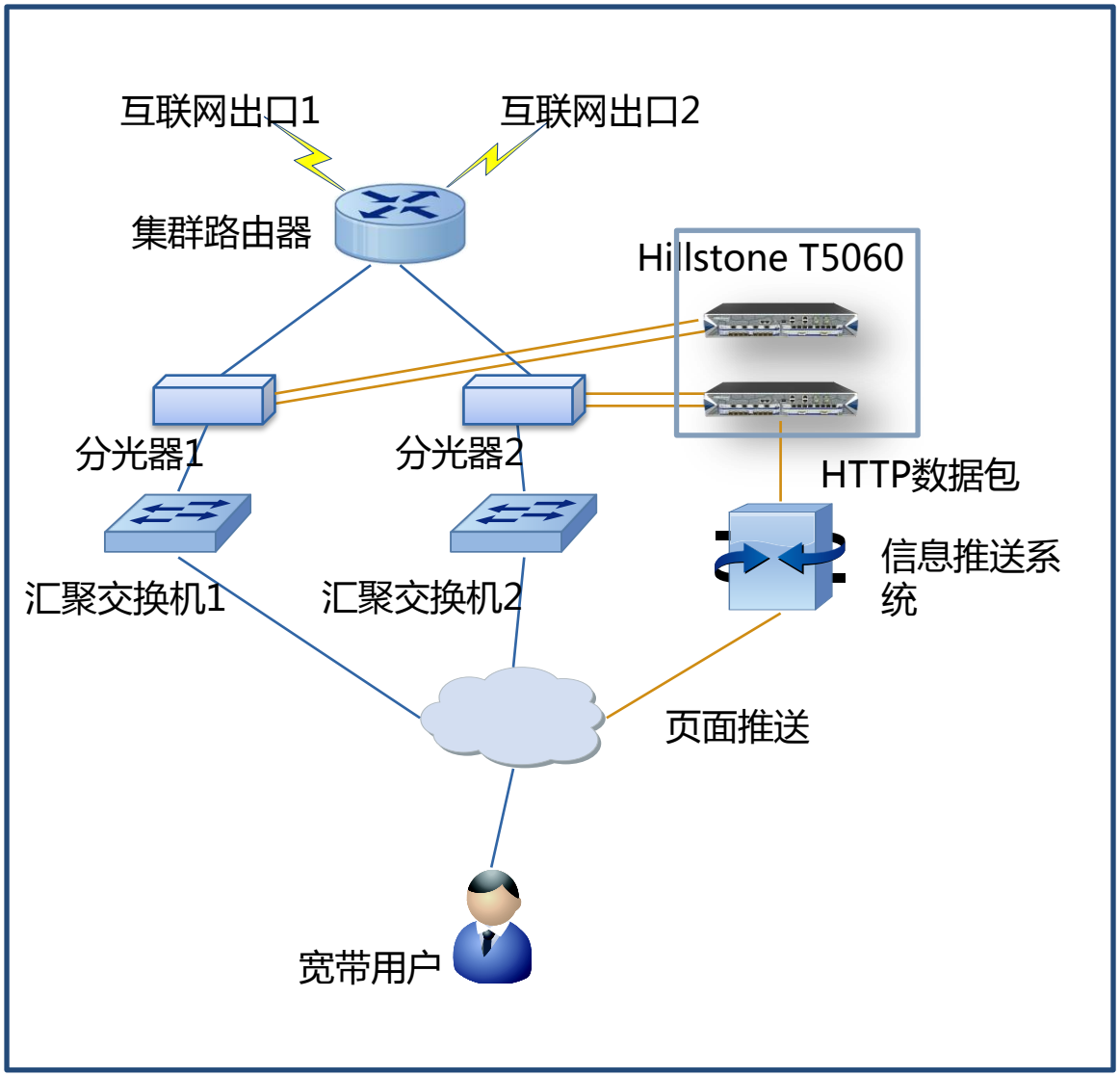
主动检测威胁、服务、网络、资源的状态信息



海量数据挖掘

网络健康指数，展现风险趋势并及时预警

案例2：在某高校互联网出口



- ✓ 10~15G业务实际流量
- ✓ 50,000并发访问用户
- ✓ 需要了解各个学区、各类应用的流量占比状态
- ✓ 二级流控刚好从IP组和应用组两个维度，提供了流量分析和统计功能
- ✓ 定期输出报表，协助高校合理规划链路带宽

山石云时代完整的智能防御平台

谢谢