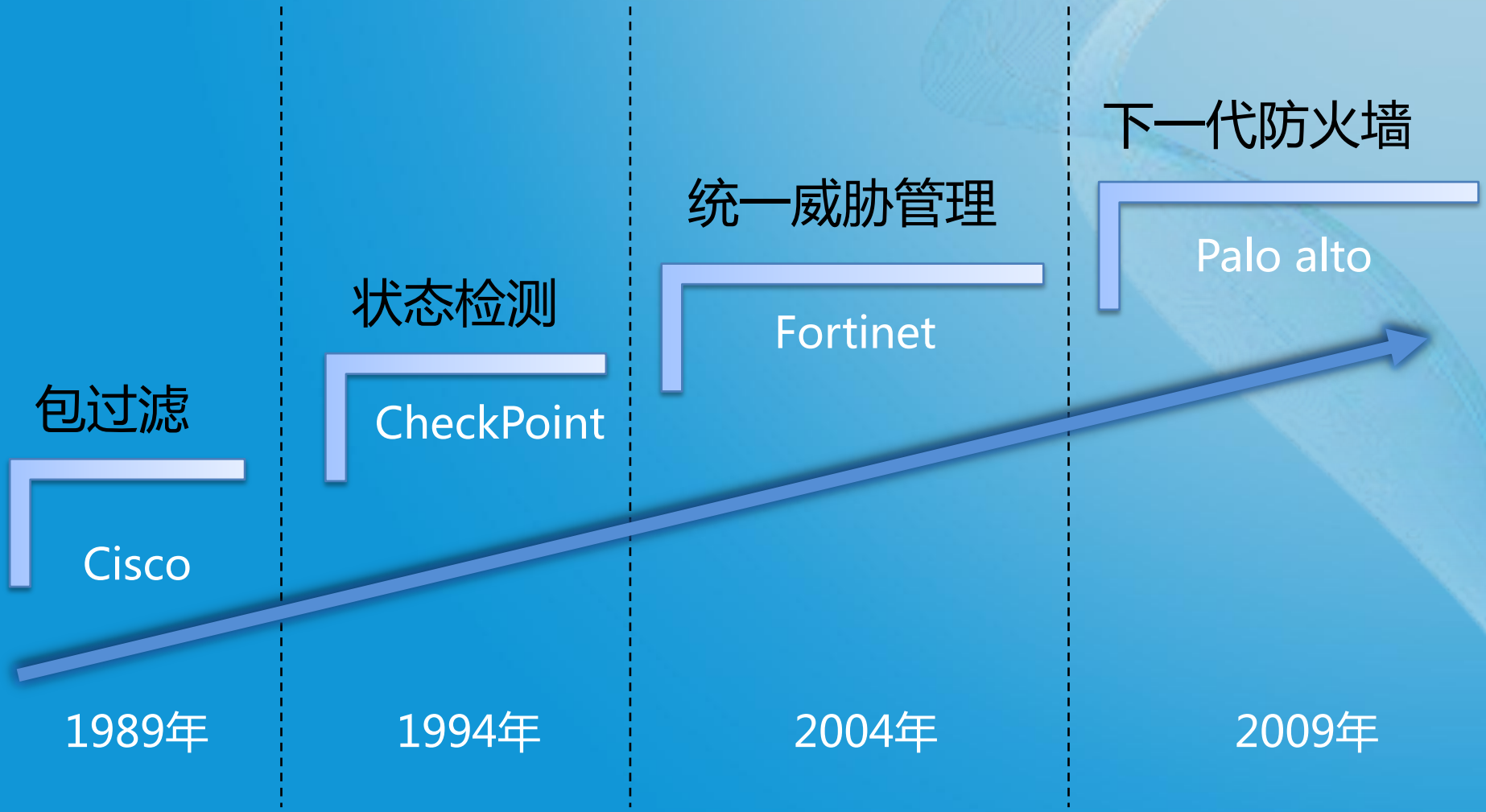
Hillstone NETWORKS

智能安全网关的发展趋势

副总裁 杨庆华

防火墙的演变史


包过滤
Cisco
1989年
状态检测
CheckPoint
1994年
统一威胁管理
Fortinet
2004年
下一代防火墙
Palo alto
2009年

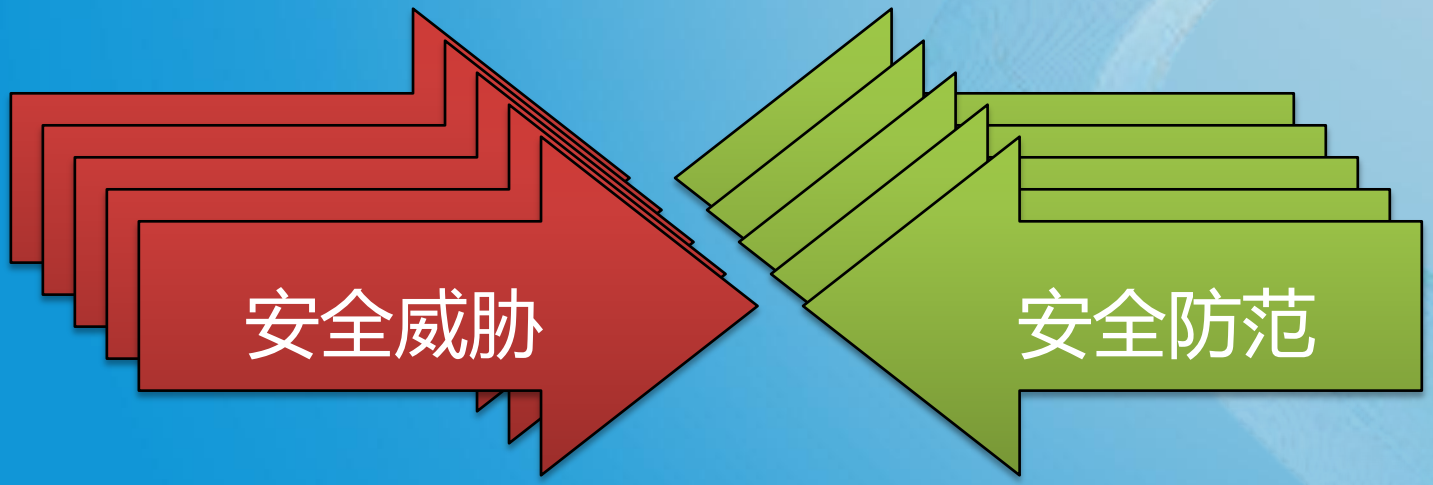
安全事件依然严重

这些公司：

受到不同程度的安全攻击并

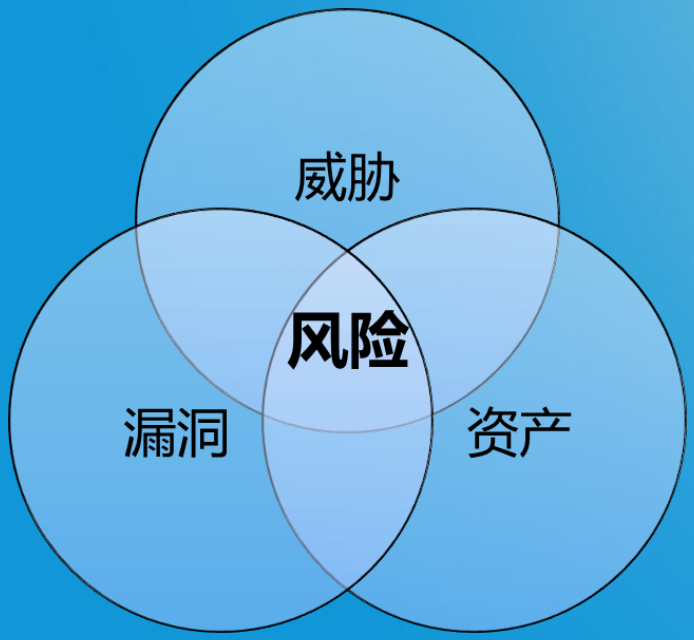
造成不同程度的损害

基于威胁的安全防护存在不足



- ？安全威胁越来越多，不断**增加安全投入**
- ？这些威胁是否真的会形成安全事件并**需要防范**
- ？需要保护的对象是否**值得**这些安全**投入**

从基于威胁到基于风险



安全风险=资产x威胁x漏洞

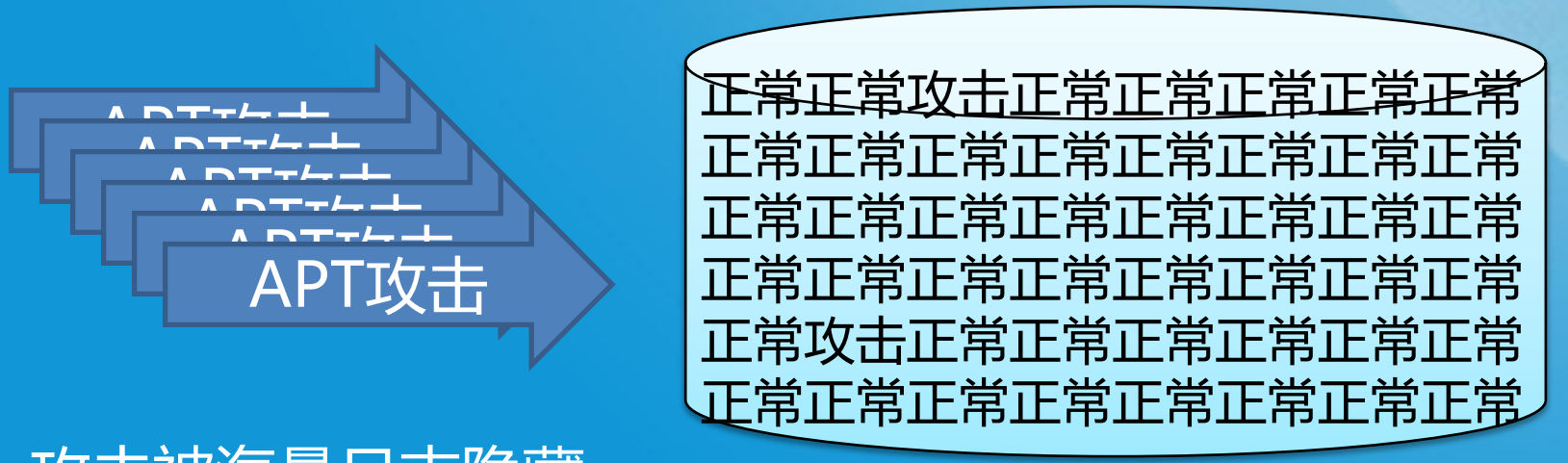
安全风险

决定

安全投资

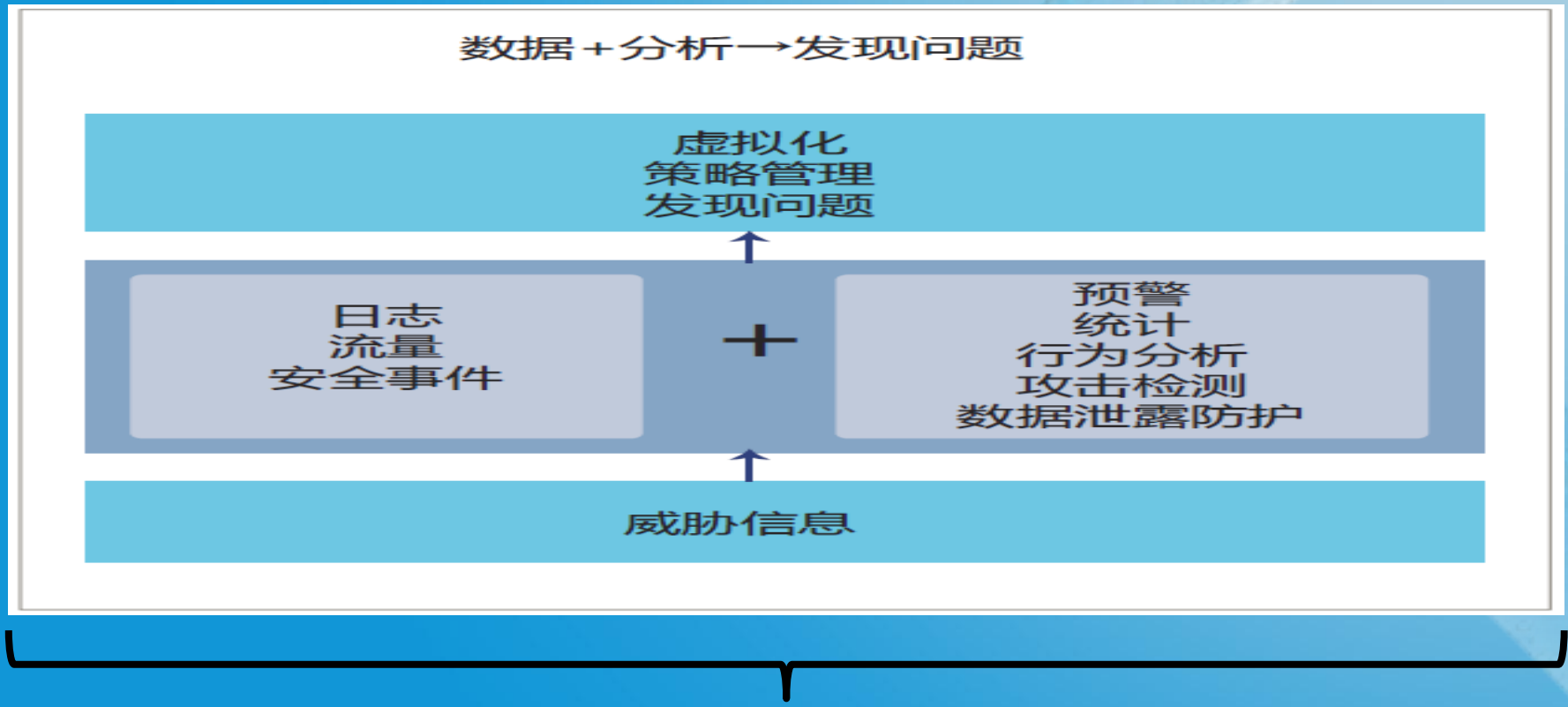
基于特征的安全分析也存在不足

无法识别特征



攻击被海量日志隐藏

利用大数据技术实施安全分析



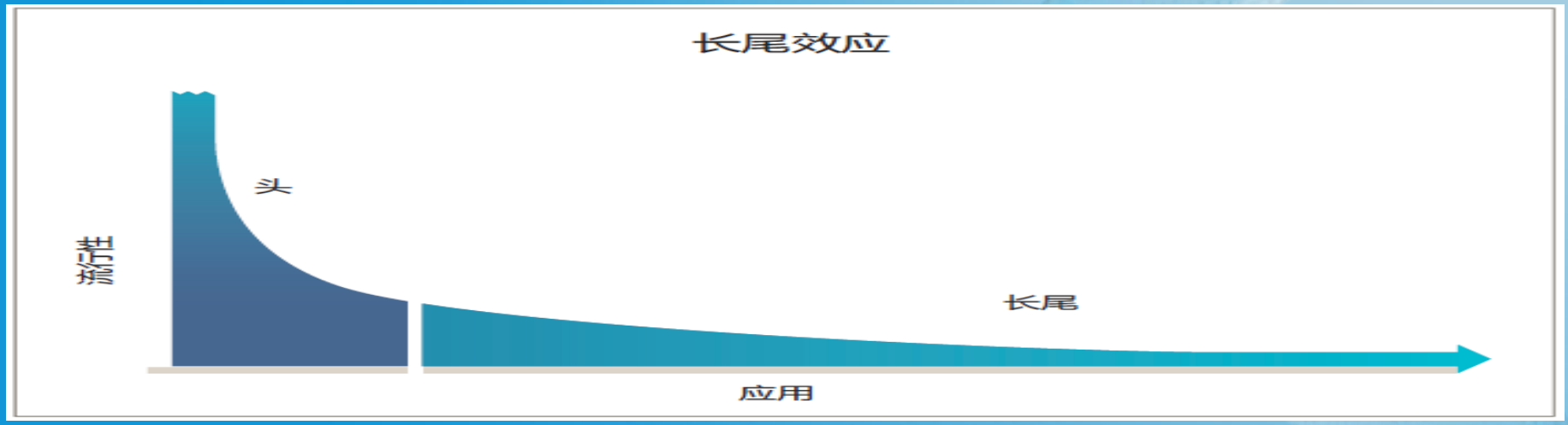
SIEM（安全信息和事件管理系统）

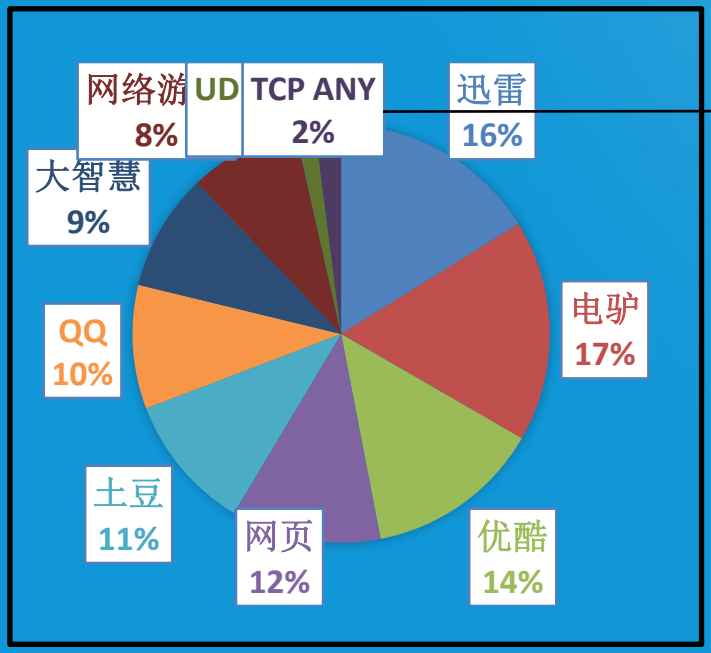
SIEM属于事后分析,且无法对安全策略进行反馈和调整

NGFW无法根据行为调整安全策略

- NGFW可以
  - 识别应用、用户、内容并实施安全控制
- NGFW不可以
  - 将用户行为关联到流量和其他事件上
  - 从时间维度上分析收集到的信息
  - 关注流量中的异常

NGFW无法规避应用的长尾效应

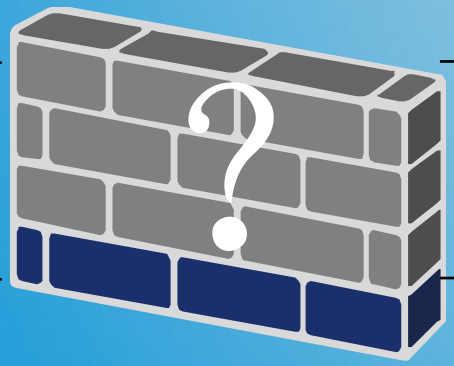




由于无法识别所有应用，一些应用被标柱为TCP ANY & UDP ANY，这些应用虽然占比很小，但隐含的安全风险可能会更大，因为NGFW对这些应用几乎没有针对性的安全控制！

NGFW无法分析加密流量

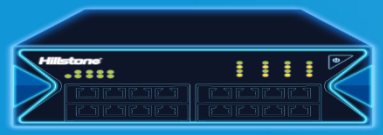
&&*¥#@¥%&
%¥@！#¥#@



&&*¥#@¥%&
%¥@！#¥#@

- 某些类型的加密传输（如SSL和SSH）内容是可能被解密的
- 不能识别的流量只能被整体的全部允许或拒绝
- 有加密流量的应用的大量使用还可能影响系统的风险级别

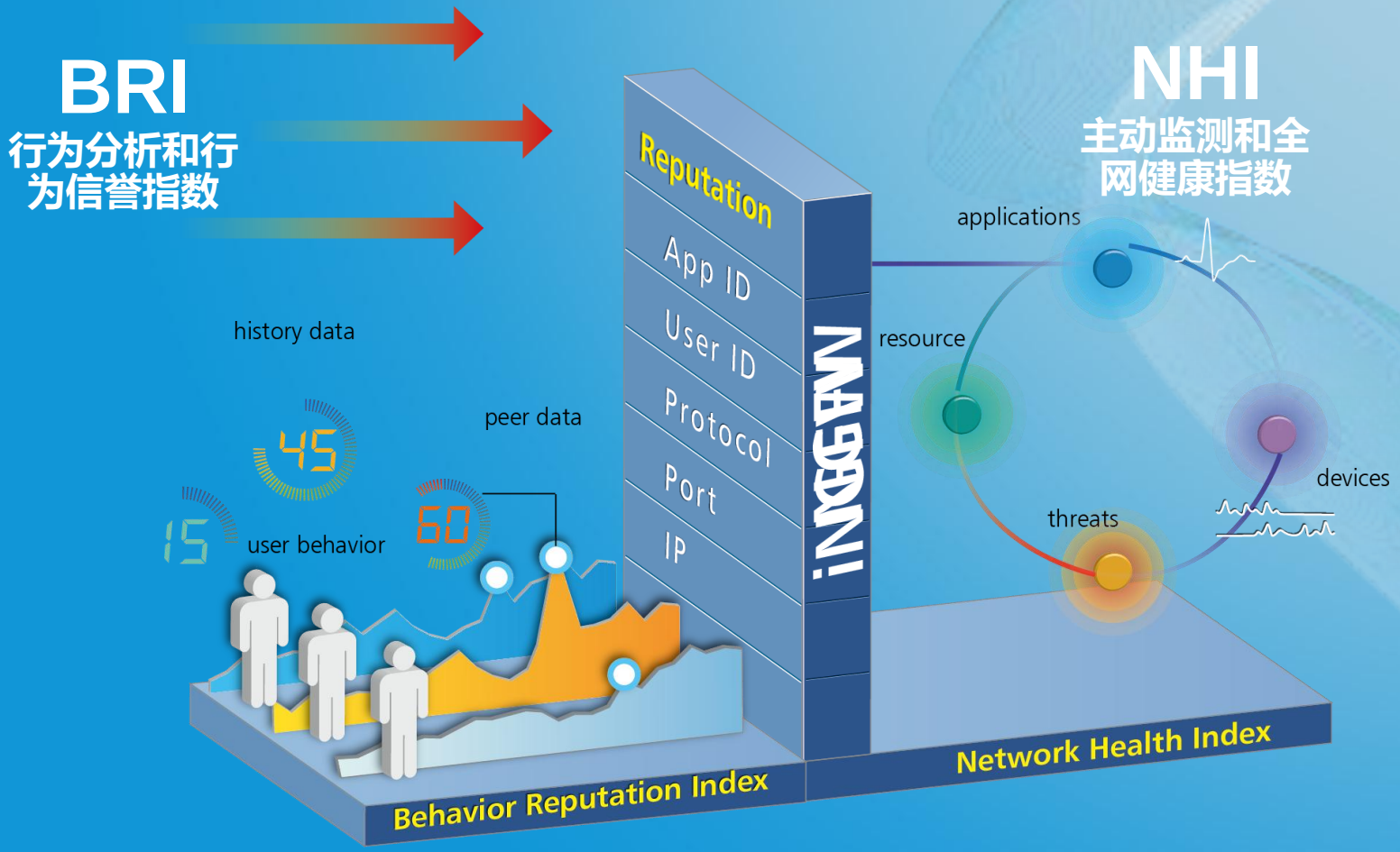
智能可以帮助您实现更多的



下一代智能防火墙

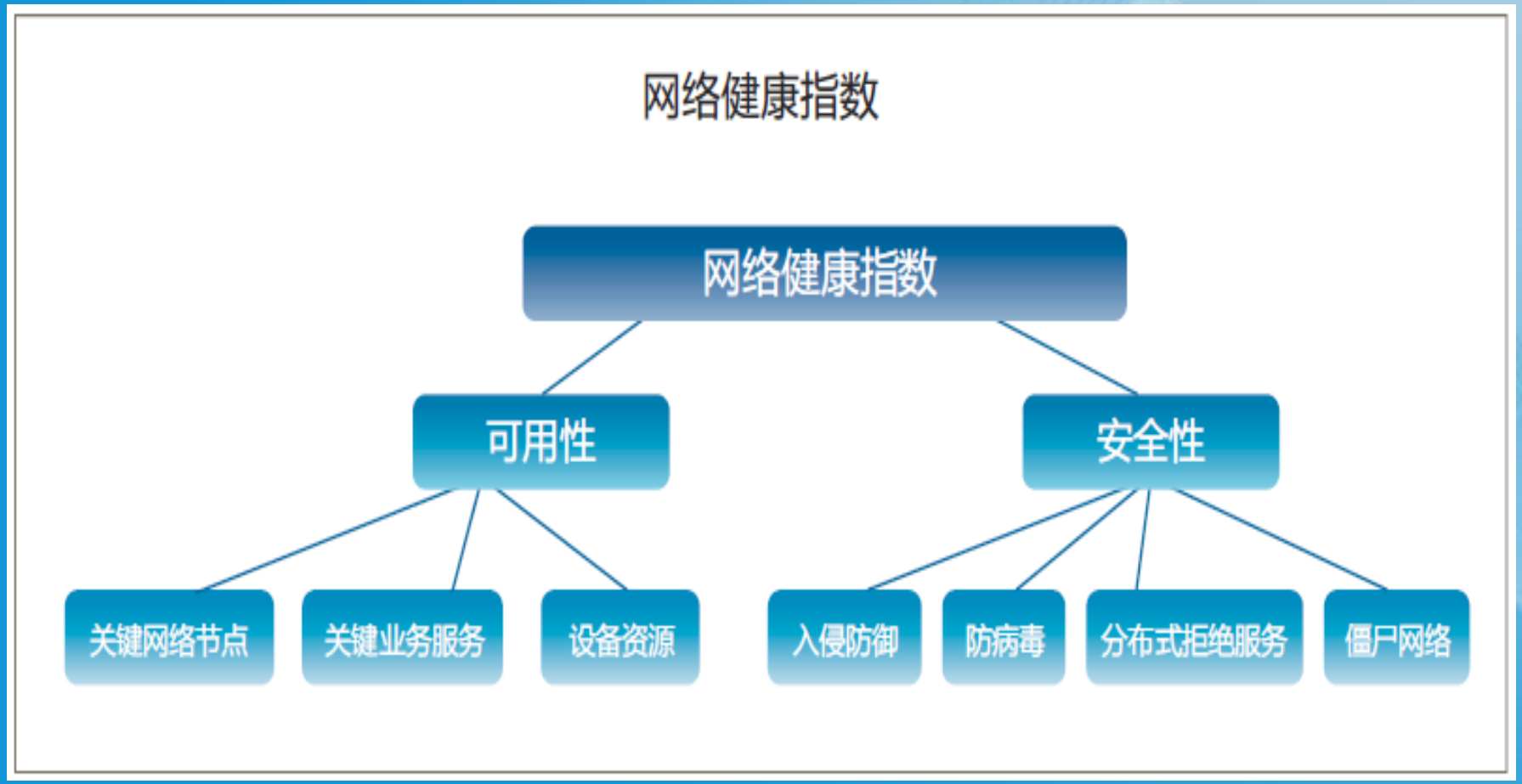
- 主动检测网络状态
- 主动检测资源状态
- 提供安全风险报告
- 动态调整安全策略
- 更智能的iQoS
- 风险评估结果可视化

下一代智能防火墙



Intelligent NGFW

主动检测和全网健康指数NHI



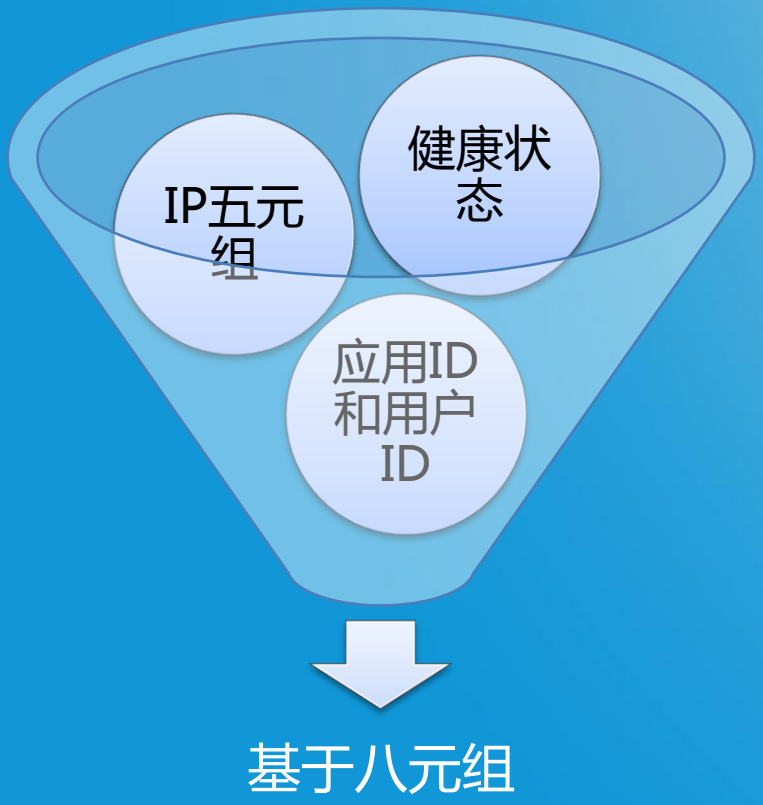
全网健康指数NHI

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

行为分析和行为信誉指数BRI

数据分析系统实时的处理安全数据，分析与内网用户、主机和服务相关的风险。内网对象的风险级别是通过行为信誉指数（BRI）呈现的，这个风险级别也可以动态影响对内网对象所实施的安全策略

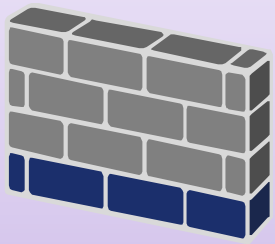
基于信誉的访问控制



企业可以利用基于信誉的访问控制为处于不同健康状态的用户设计不同的策略：

- ✓处于危险状态的用户，应进行隔离并分配到需要修复的网络中，或提供类似于网络访客级别的访问；
- ✓处于亚健康状态的用户，应禁止访问网络中敏感或高度保密的资源；
- ✓ 如果由于健康状态导致访问受到限制，应通过终端代理或网页弹出框通知用户

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**

下一代智能防火墙带给我们什么

降低安全管理的门槛和风险，减少安全管理和运营的费用

安全防范	应激响应 →	主动管理
安全事件分析	人工挖掘 →	智能分析
安全事件报告	孤立的事件报告 →	多维度风险分析和健康报告
安全规则配置	静态规则 →	动态规则

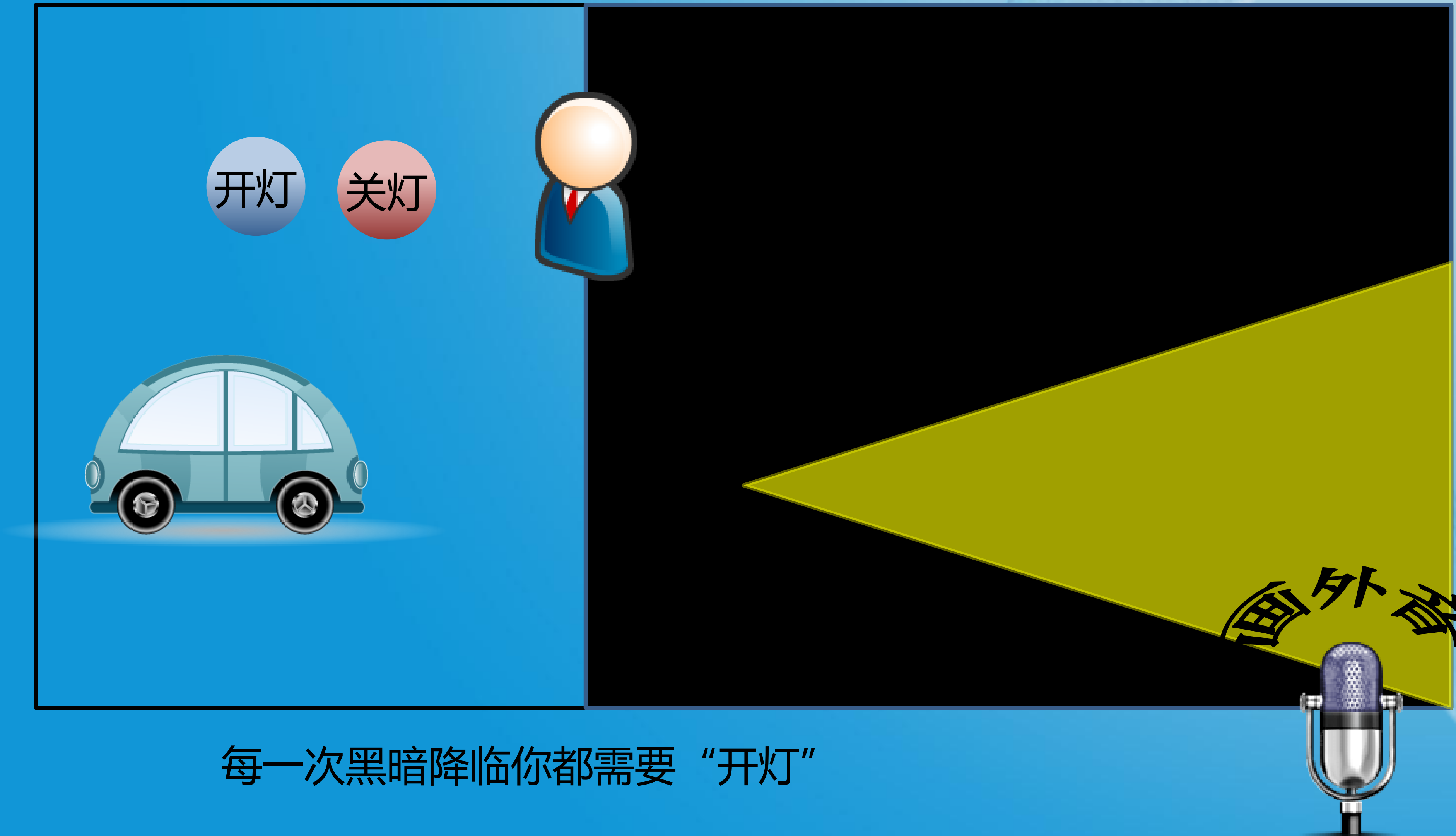
安全事件防范的应激响应

直到跑偏时你才知道轮胎被扎

安全事件防范的主动管理

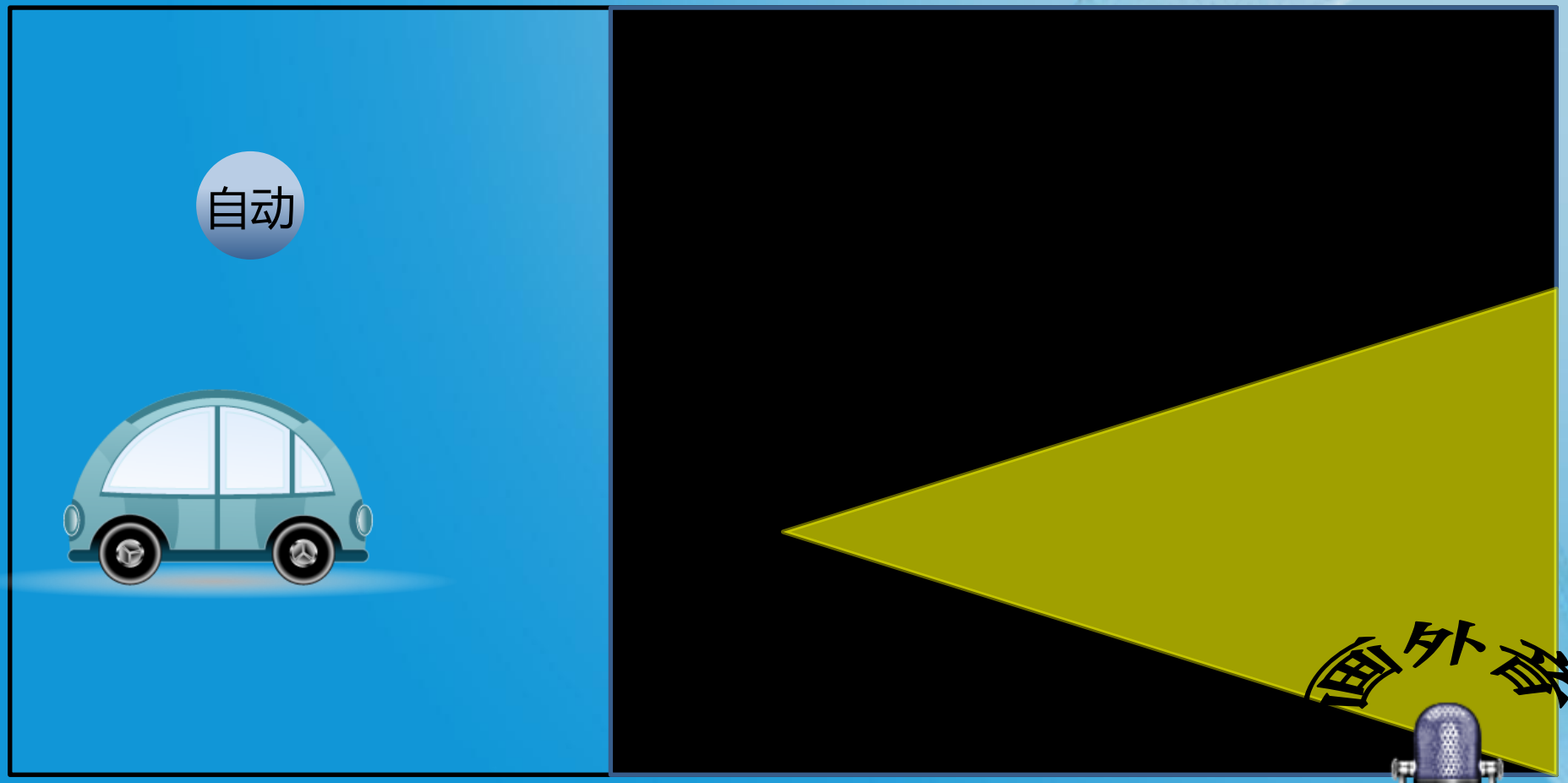
当轮胎稍有亏气时就能得到预警

安全规则配置的静态规则



每一次黑暗降临你都需要“开灯”

安全规则配置的动态规则



无数次黑暗降临你只需要一次“开灯”

网络健康指数NHI

网络连通

0-100

80分

设备资源

0-100

50分

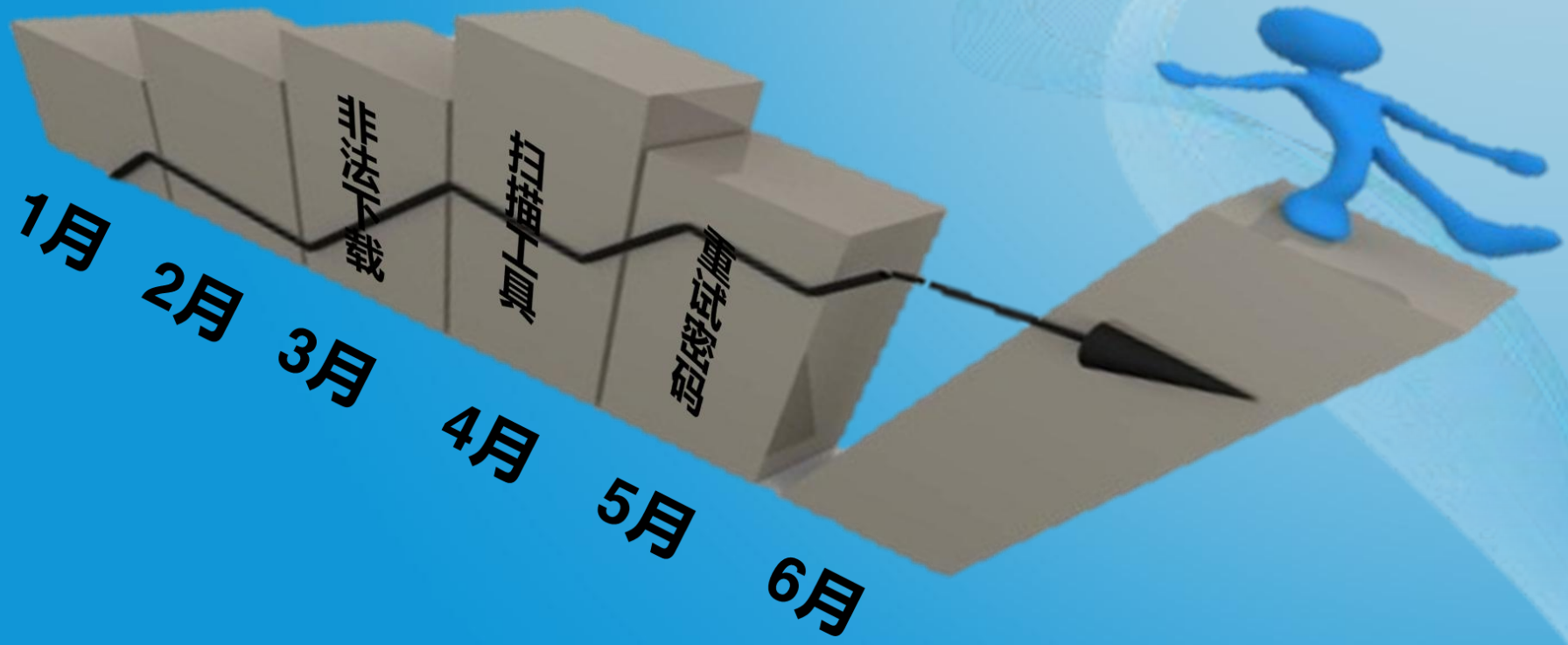
业务服务

0-100

30分

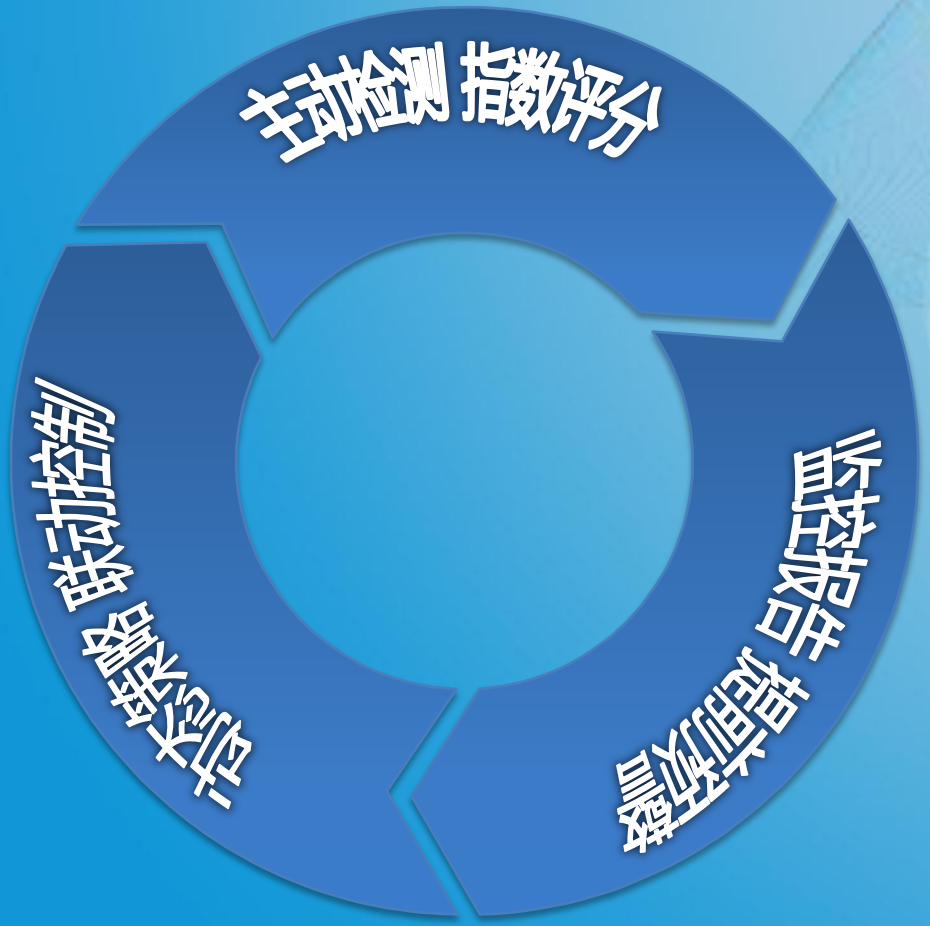
30分

行为信誉指数BRI



50分 行为信誉指数

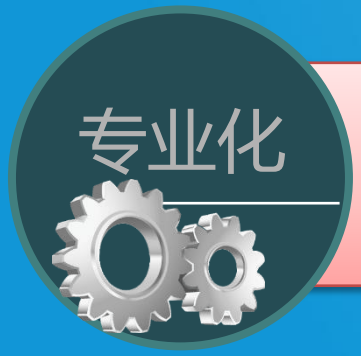
下一代智能防火墙的联动控制



创新的网络安全方案供应商-山石网科

Hillstone NETWORKS

- 网络安全市场前三甲
- 引领高性能安全
- 首创智能安全



- 专注于安全技术
- 几十项专利及软件著作权
- 创始团队来自世界级知名企业

- 北京、苏州、美国研发中心快速响应
- 20个办事机构近距离接触客户
- 千名认证工程师本地化服务

不断追求创新

2006

2007
Hillstone在北京成立

2008
发布业界第一个基于多核平台的64位实时并行安全操作系统

发布万兆多核安全网关

2010
发布新一代多核Plus G2安全架构

发布100G高性能数据中心防火墙

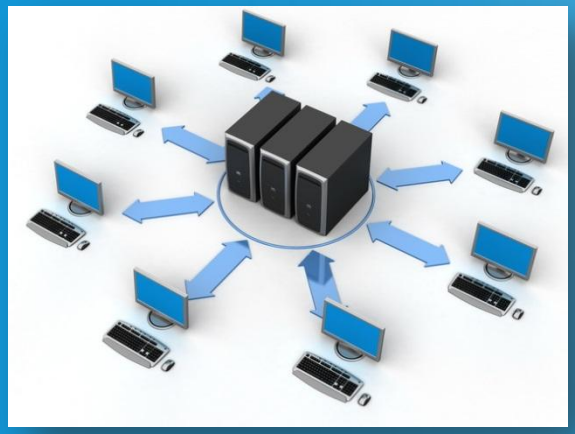
2012
苏州研发中心成立
绿色节能、支持虚拟化云数据中心防火墙

美国研发中心成立
发布业界首款32核产品

下一代智能防火墙


清華大學
Tsinghua University
北京大學
PEKING UNIVERSITY
中国科学技术大学
University of Science and Technology of China
南開大學
天津大學
Tianjin University
東南大學
武漢大學
上海交通大學
SHANGHAI JIAO TONG UNIVERSITY
中國人民大學
中山大學
SUN YAT-SEN UNIVERSITY
華南理工大學
South China University of Technology
西安交通大學
XI'AN JIAOTONG UNIVERSITY
哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
華中科技大學
HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY
西北工業大學
NORTHWESTERN POLYTECHNICAL UNIVERSITY
中國海洋大學
北京理工大学
北京師範大學
BEIJING NORMAL UNIVERSITY
中央財经大学
Central University of Finance and Economics
北京郵電大學
Beijing University of Posts and Telecommunications
北京科技大学
University of Science and Technology Beijing

教育行业案例



150多所高校，50多所211工程院校、20多所985高校选择Hillstone

近10个市级教育城域网，近万所中小学，部署Hillstone

近100个其他教育科研机构成为Hillstone的用户

智能引领未来

高级威胁和0-day攻击的本质是高度可规避检测，导致基于特征的防护越来越无计可施。安全保护模式正在从基于威胁的保护向基于风险的保护转变。

智能关联分析

全网健康指数

基于信誉的访问控制

用户行为信誉指数

感知风险提前预警

THANK YOU !

如有问题，请联系我们
服务热线： 400-828-6655
www.hillstonenet.com.cn