新型威胁的智能化防御

演讲人：张凌龄

职务：山石网科市场副总裁

日期：2014-9-25

安全事件依然严重

2014.8 俄国黑客组织盗取

被境外通过植入后门控制

用户名、密码

被境外服务器控制

网站被刷库

2013年较2012年新增

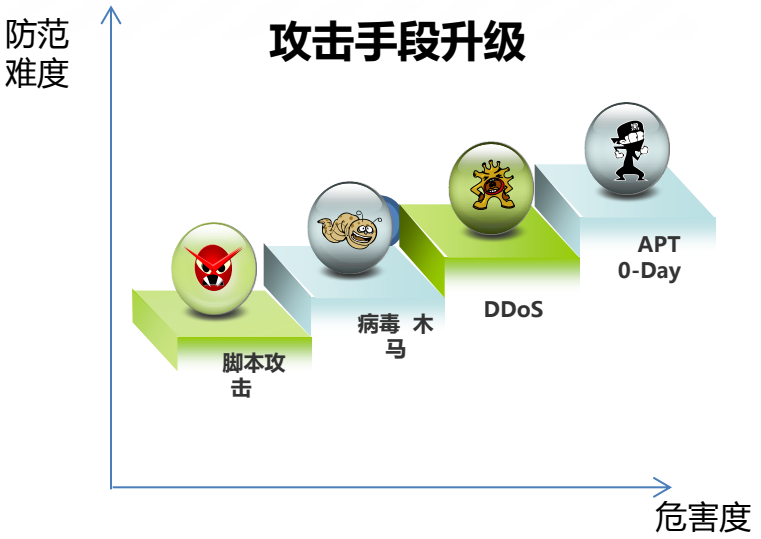
多电子邮件地址

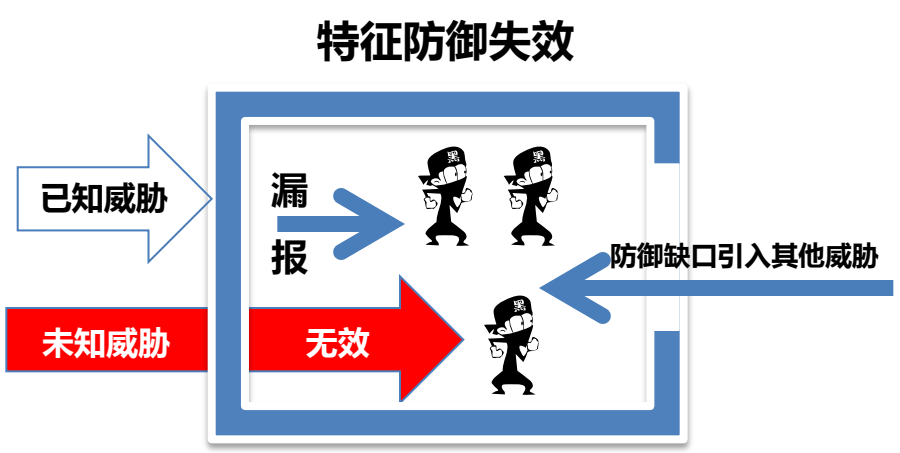
2013.8.13我国

遭攻击瘫痪

- 中国互联网发展报告2014

老办法覆盖不了的新问题





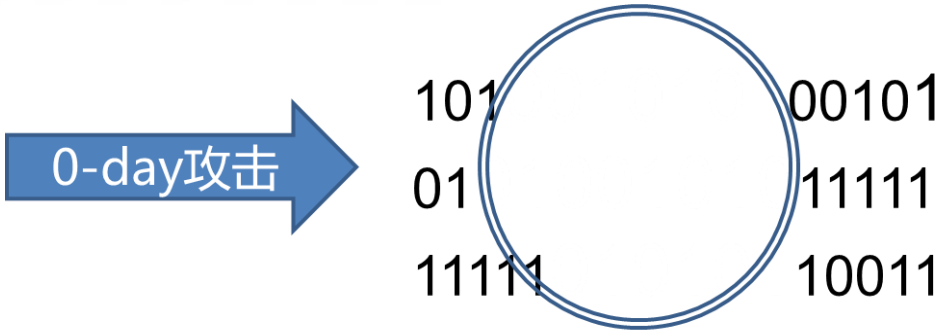
技术瓶颈

- 已知威胁：特征覆盖不可能达到100%，总有漏掉的攻击行为；
- 未知威胁：传统基于模式匹配的监测方式对其无效；

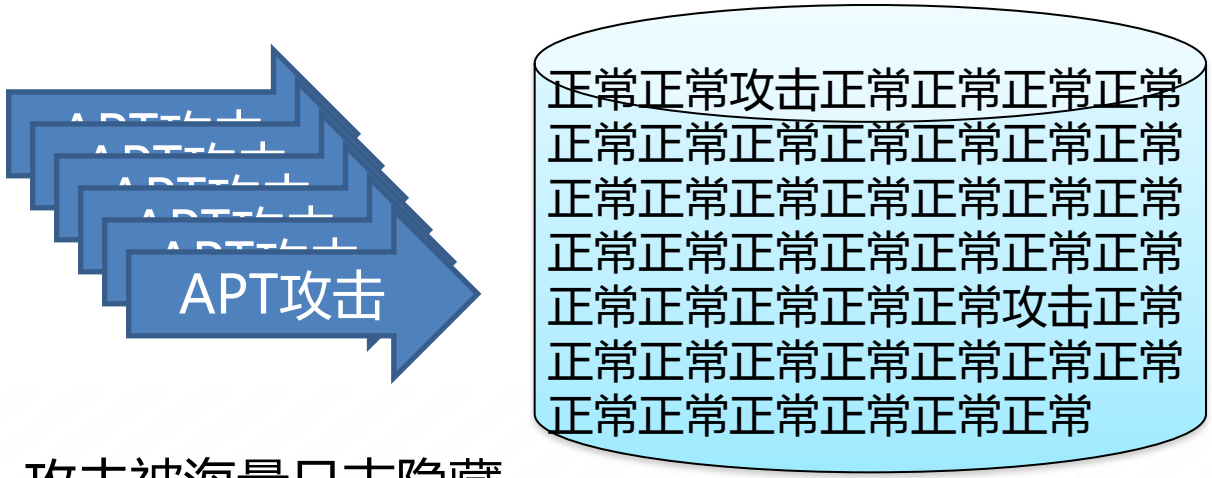
管理问题

- BYOD引入静态策略无法防护的问题；
- 被动防护难以对抗持续攻击；
- 防护时机：只关注了威胁进入瞬间；
- 防护位置：只关注了边界点安全

基于特征的安全分析存在不足



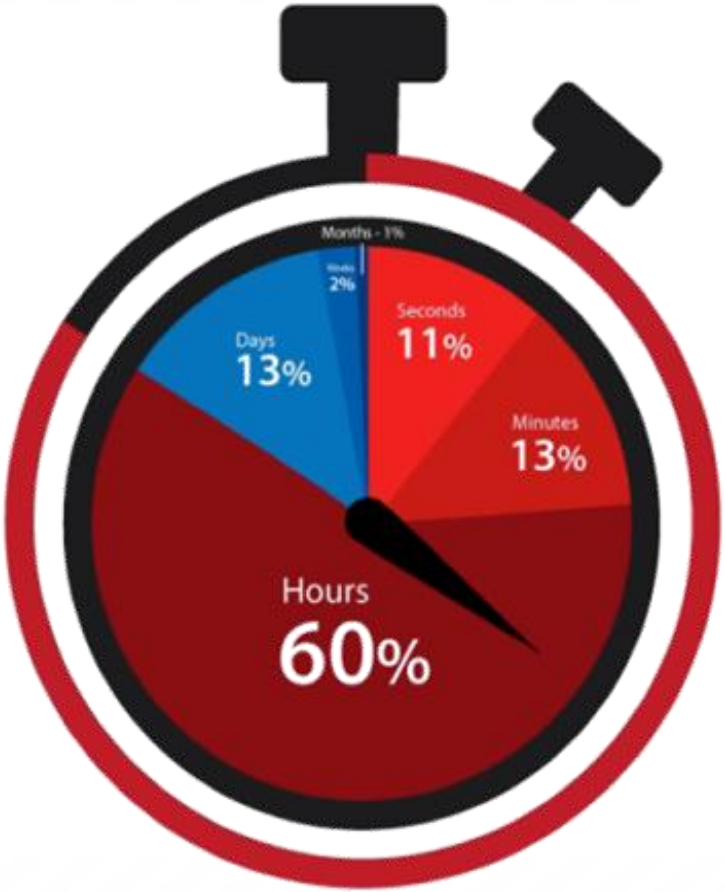
无法识别特征



攻击被海量日志隐藏

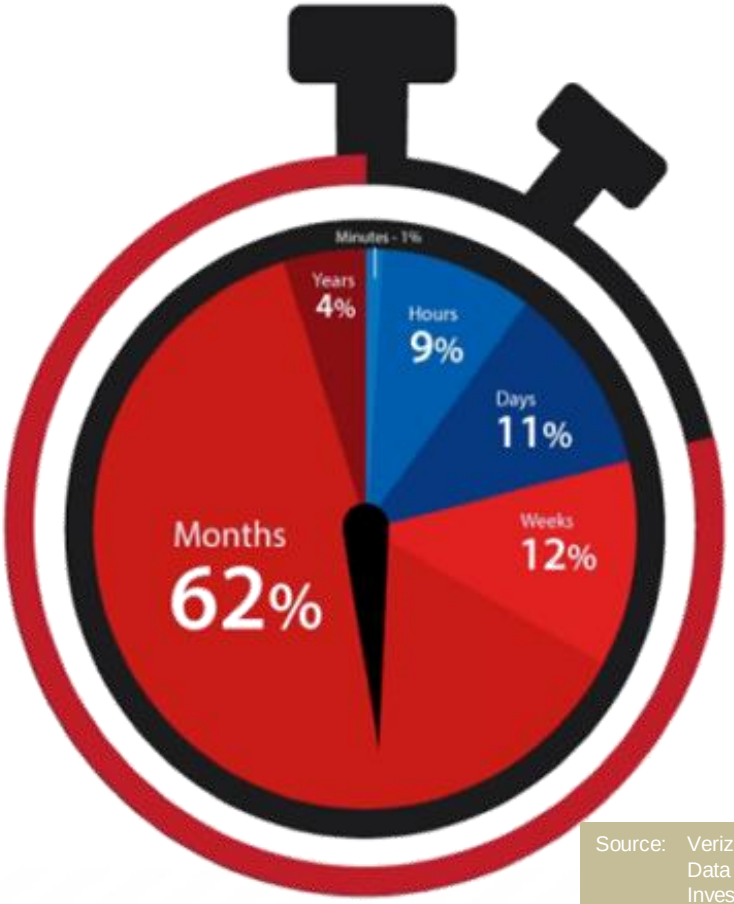
攻击发现时间

攻击到攻陷



84%

攻陷到发现

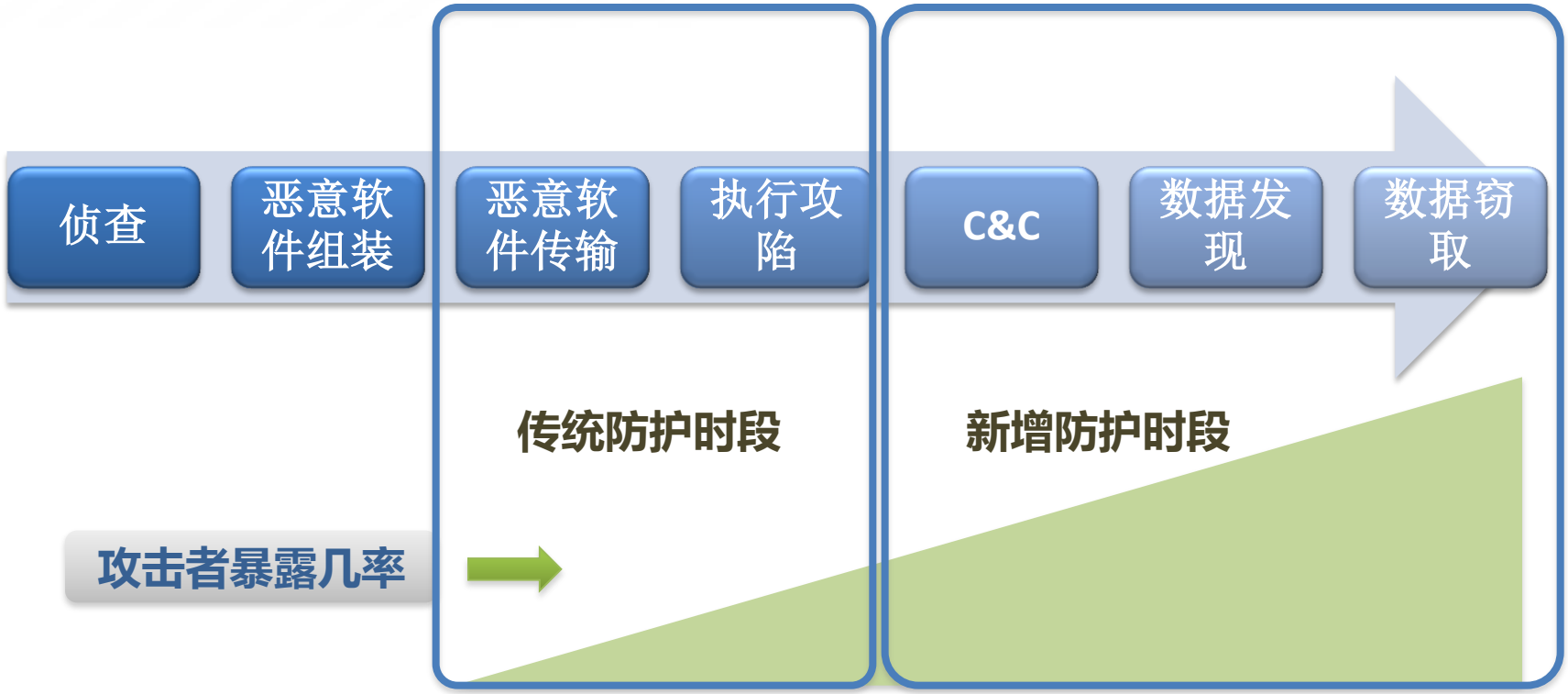


78%

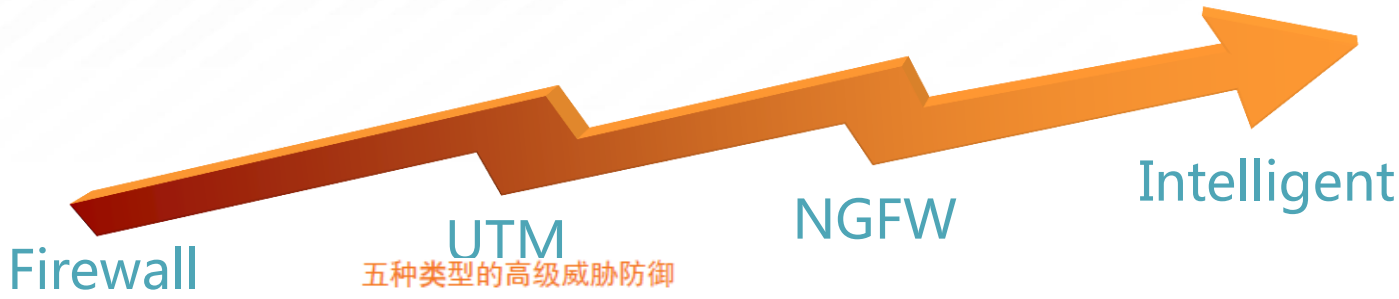
Source: Verizon 2013 Data Breach Investigations Report

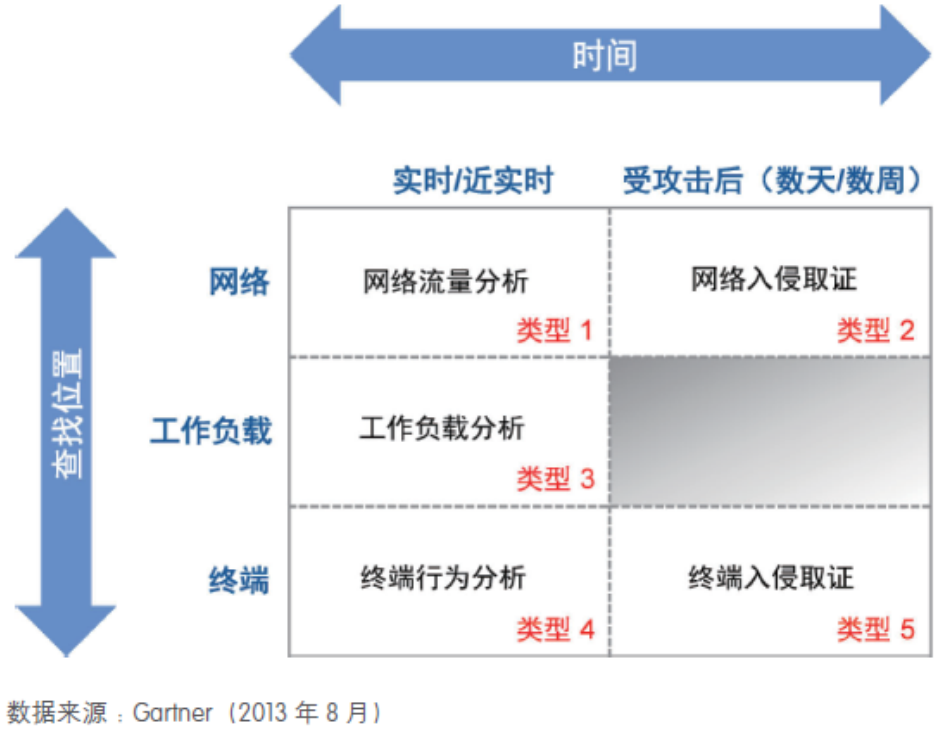
*2013 Verizon DBIR

攻击检测点



下一代网络安全解决方案

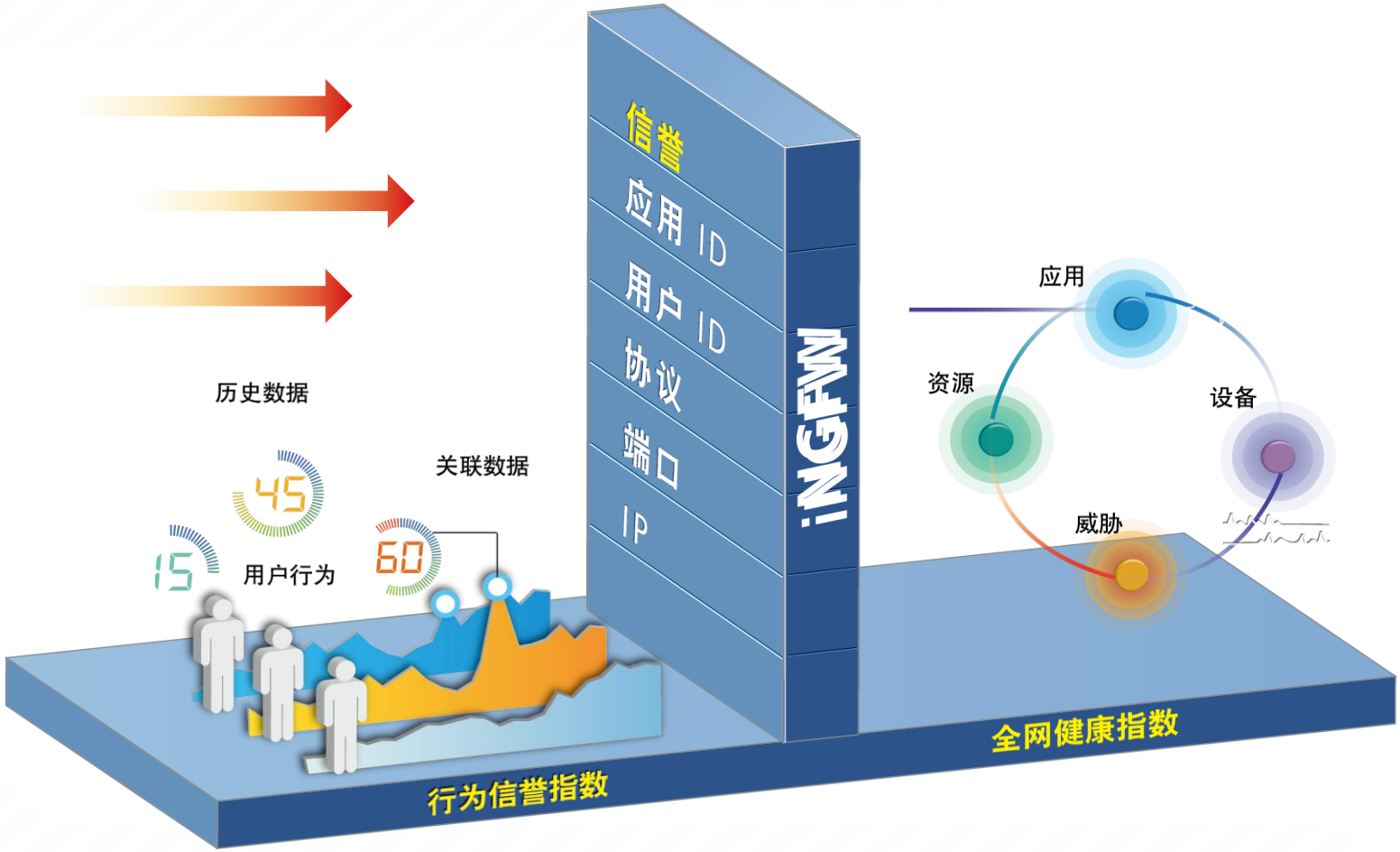




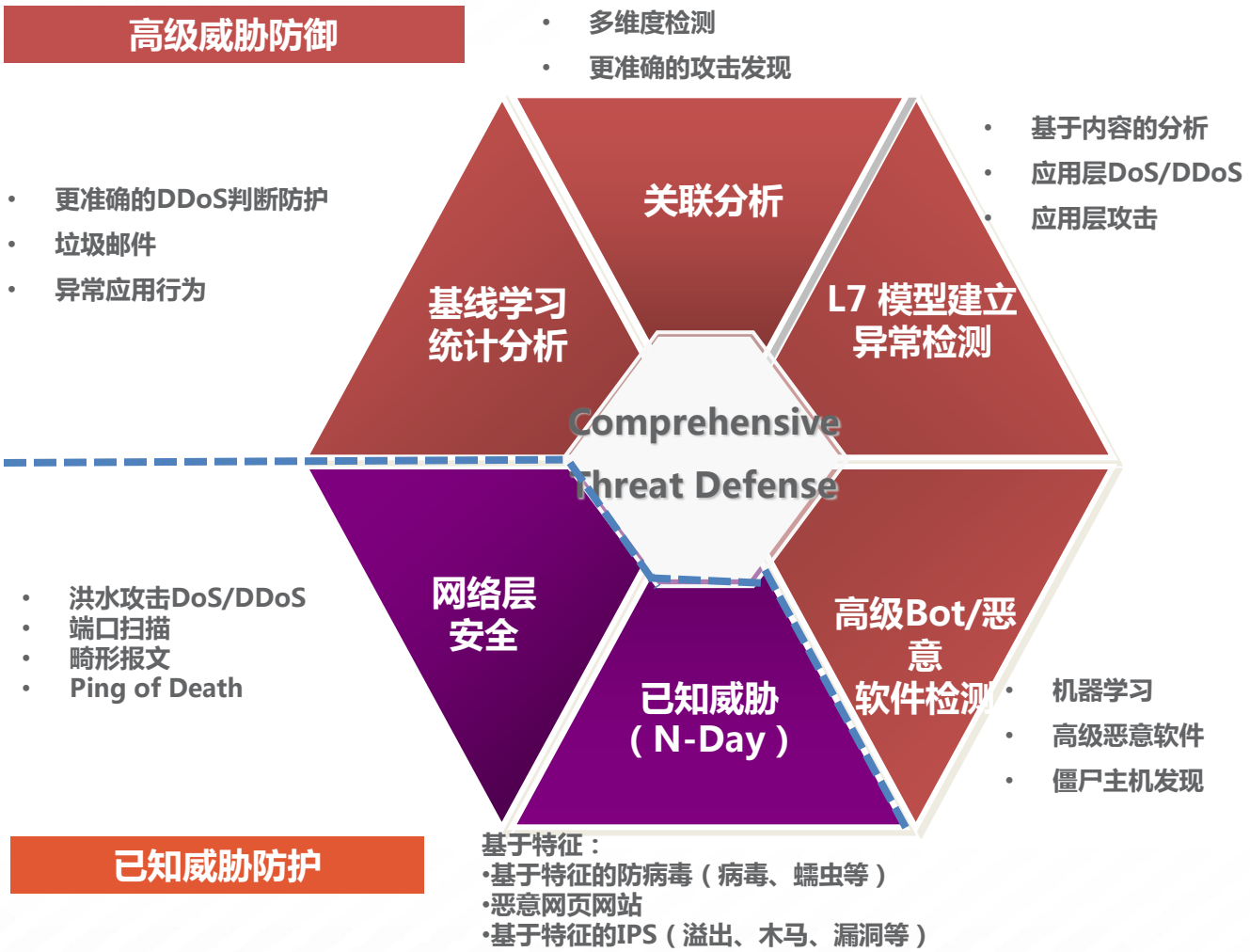
数据来源：Gartner（2013 年 8 月）

预测，阻挡，检测，调控等全方位、全生命周期的监控

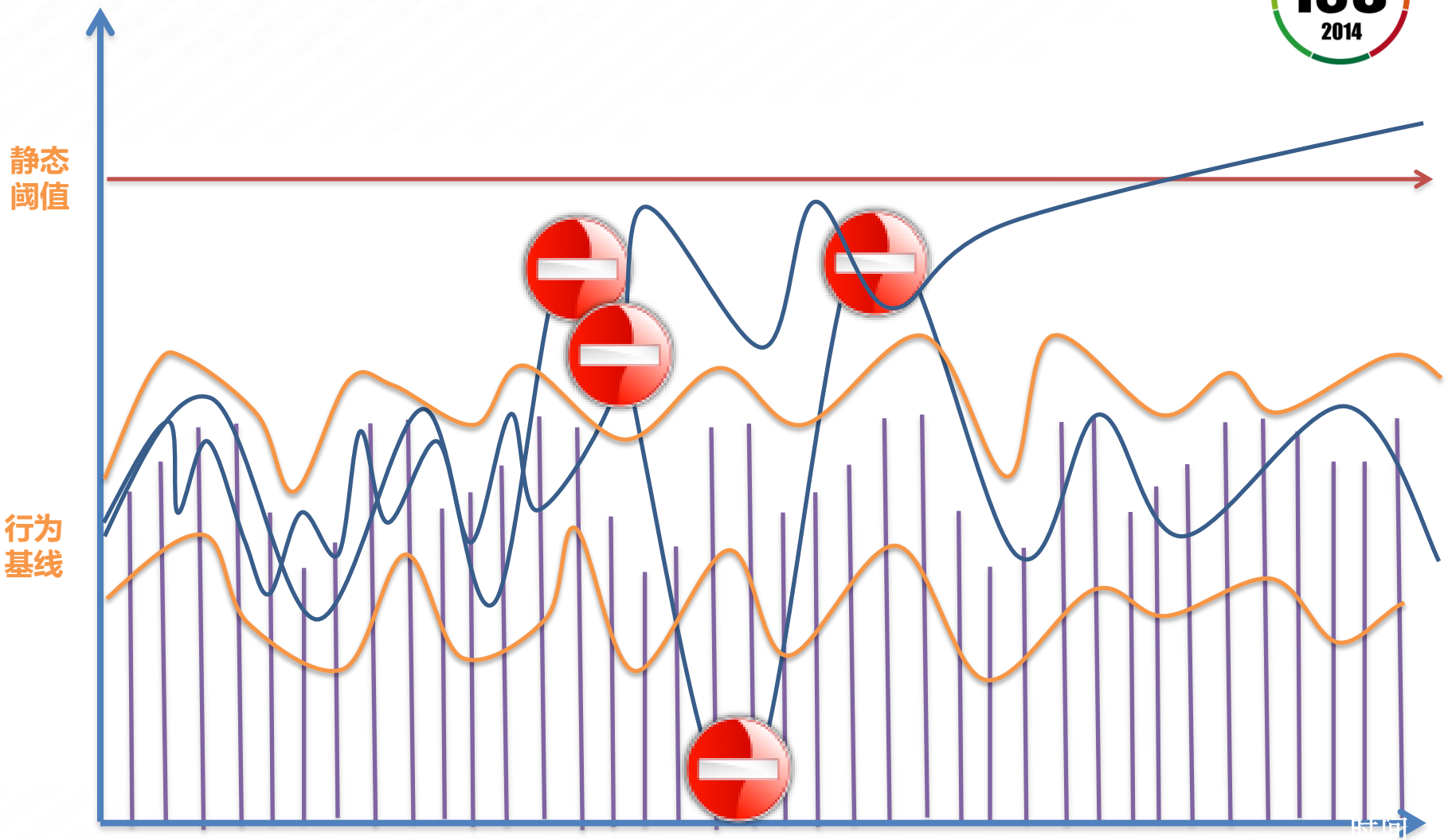
山石网科下一代智能防火墙



高级威胁防御

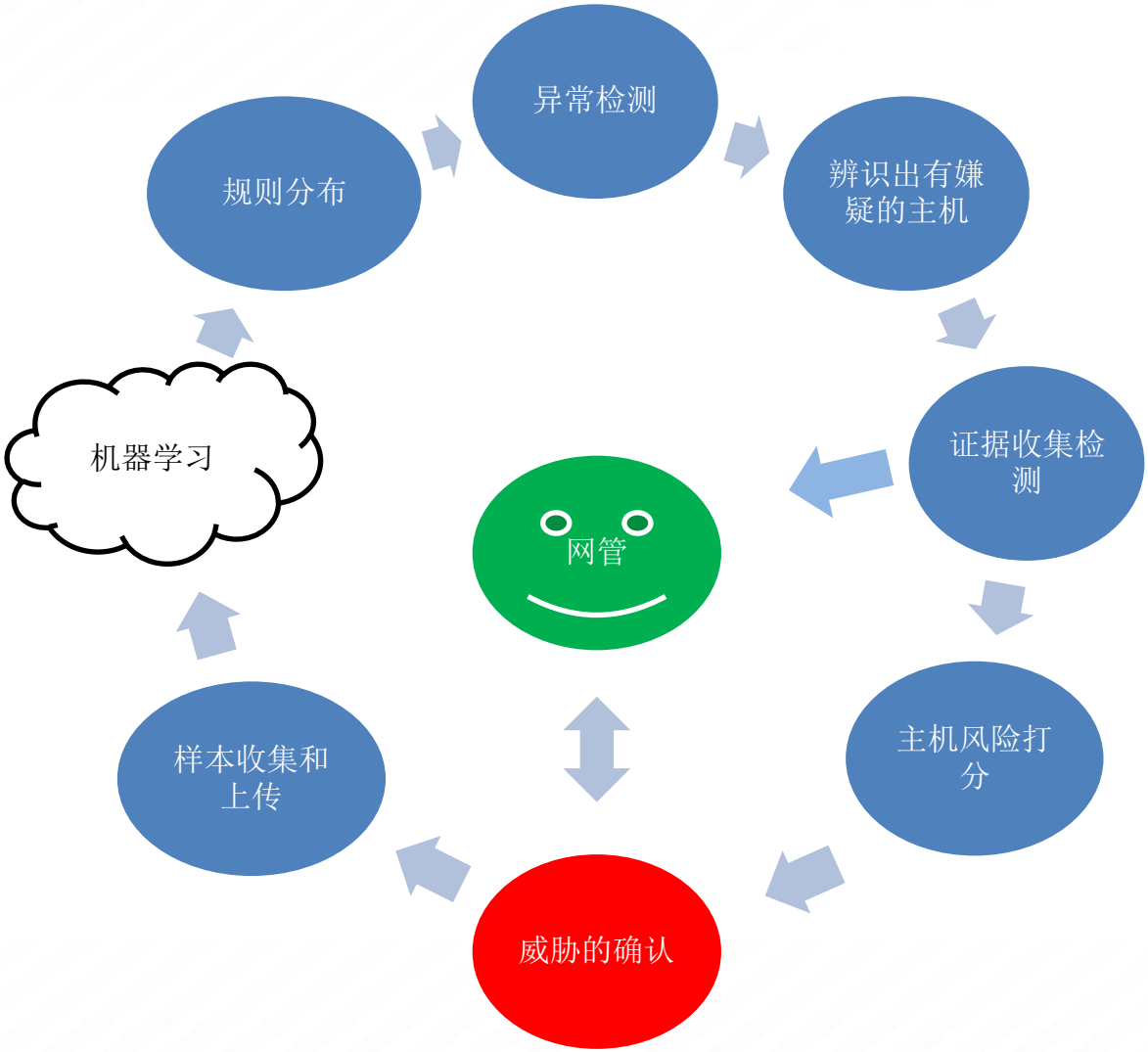

高级威胁防御
多维度检测
更准确的攻击发现
更准确的DDoS判断防护
垃圾邮件
异常应用行为
关联分析
基线学习
统计分析
L7 模型建立
异常检测
基于内容的分析
应用层DoS/DDoS
应用层攻击
Comprehensive
Threat Defense
网络层
安全
洪水攻击DoS/DDoS
端口扫描
畸形报文
Ping of Death
已知威胁
(N-Day)
高级Bot/恶意
软件检测
机器学习
高级恶意软件
僵尸主机发现
已知威胁防护
基于特征：
•基于特征的防病毒（病毒、蠕虫等）
•恶意网页网站
•基于特征的IPS（溢出、木马、漏洞等）

行为基线和特征分析示意



通过动态行为基线和行为特征来更早更准发现异常

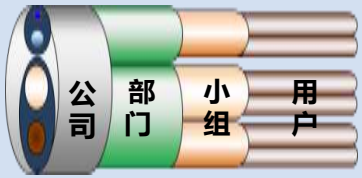
山石网科智能安全理论模型



增强的下一代防火墙功能

用户及应用识别

多维威胁检测



智能流量管理iQoS

可视化运维管理

全面提升用户体验

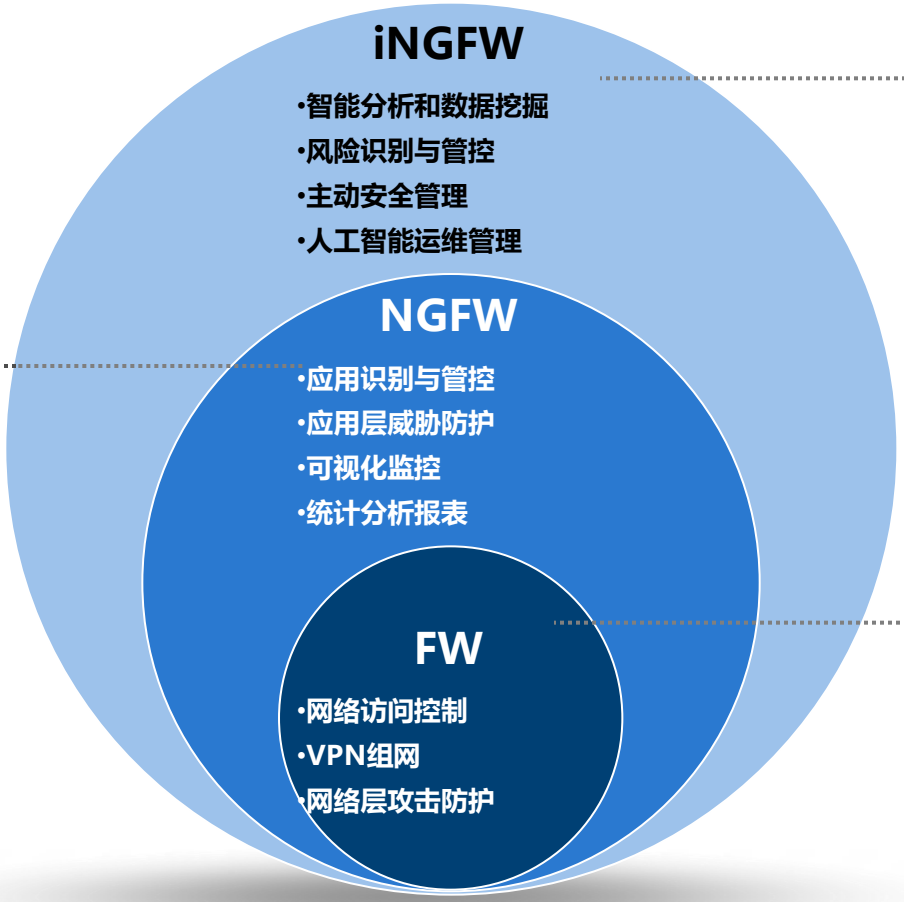
山石带来的新价值

- 检测特征无法识别威胁
- 检测阈值无法识别威胁
- 全面的2-7层威胁防护
- 提前发现威胁并进行预警

- 实时掌握业务的可用性
- 安全风险提前防范
- 全网健康报告提升管理体验

- 用户、应用和网络全面可视化
- 精细化流量管理
- 全面提升运维效率

智能 就这样与众不同



高级持续威胁防护

基于风险的安全防护

动态安全管理

应用层安全防护

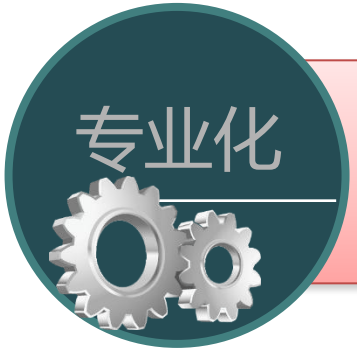
可视化运维管理

网络组网

网络层安全防护

山石网科 创新的网络安全方案供应商

- 网络安全市场前三甲
- 首创“下一代智能安全”
- 引领数据中心网络安全



- 专注于安全技术
- 几十项专利及软件著作权
- 创始团队来自Netscreen、Juniper、Cisco

- 北京、苏州、硅谷三地研发中心快速响应
- 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

ISC 2014

2006

Hillstone NETWORKS

Hillstone在北京成立

2007

Stone

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

2008

ISO 9001:2008 REGISTERED COMPANY

Multi Core G2

ISCCC 中国信息安全认证中心 China information security certification center

发布新一代多核Plus G2安全架构

2010

Tencent 腾讯

R6 READY

中国电信 CHINA TELECOM

发布100G高性能数据中心防火墙

2011

CeBIT HANNOVER 1.-5.3.2011

RSA 2011 CONFERENCE

中国移动通信 CHINA MOBILE

HUAWEI

苏州研发中心成立
绿色节能、虚拟化云数据中心防火墙

2012

RED HERRING GLOBAL WINNER 100

ICSA labs

ZTE中兴

美国研发中心成立
发布业界首款32核产品

2013

下一代智能防火墙

全并行架构360G数据中心防火墙

2014

Gartner

入选Gartner魔力象限

进军国际市场

TREND MICRO 趋势科技

合作伙伴

跻身Gartner企业级防火墙魔力象限

Figure 1. Magic Quadrant for Enterprise Network Firewalls

Source: Gartner (April 2014)

在网络安全技术的前瞻性
国内第一，国际第三

山石网科 引领网络安全新技术

Thanks!