



2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT

聚力·赋能

2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT



2016阿里安全峰会

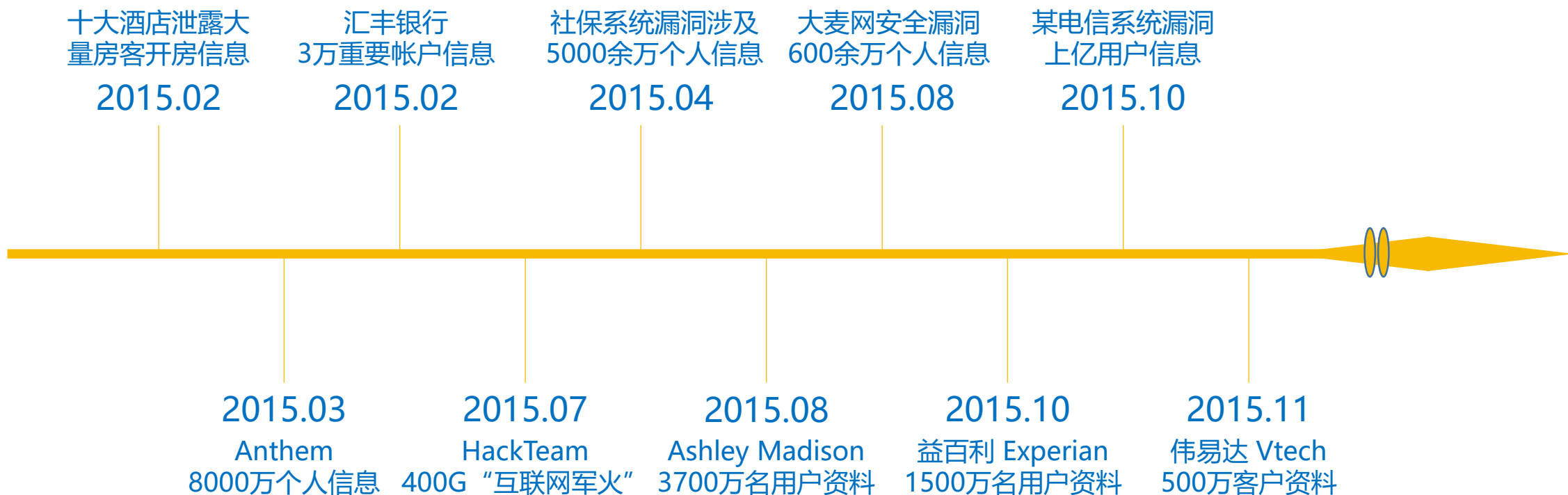
2016 ALIBABA SECURITY SUMMIT

# 数据泄露时代的 网络边界防御实践

熊瑛 @ 网康科技  
2016.7



## 回顾：2015十大信息泄漏事件

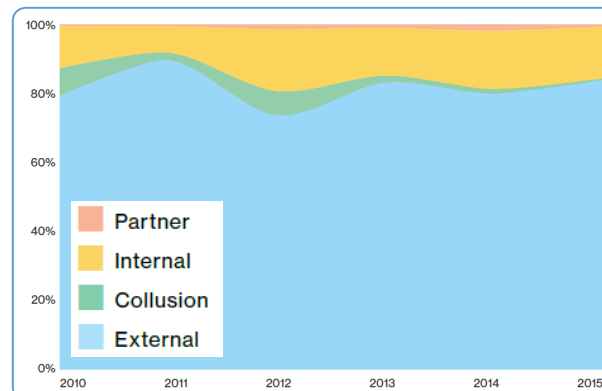


# 谁动了我的数据？

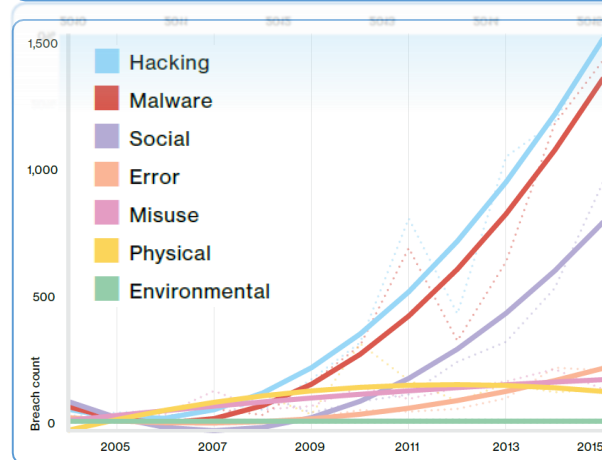
2016 Verizon Data Breach Investigations Report (DBIR)



**89%**的数据泄露事件以经济利益或间谍活动为动机



数据窃取者绝大部分来自于企业外部



常用手段

- 黑客攻击
- 恶意软件
- 社工攻击

# 为什么难以防范？

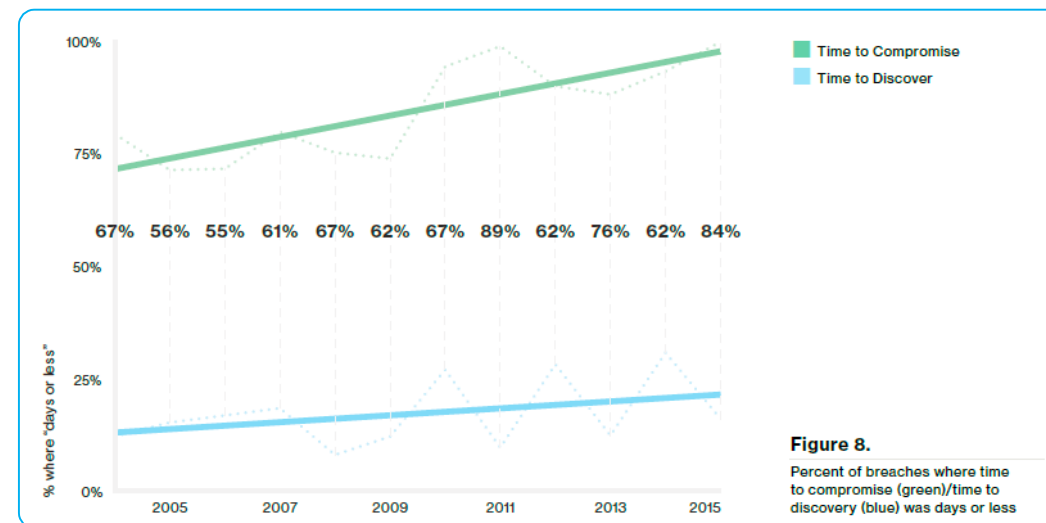
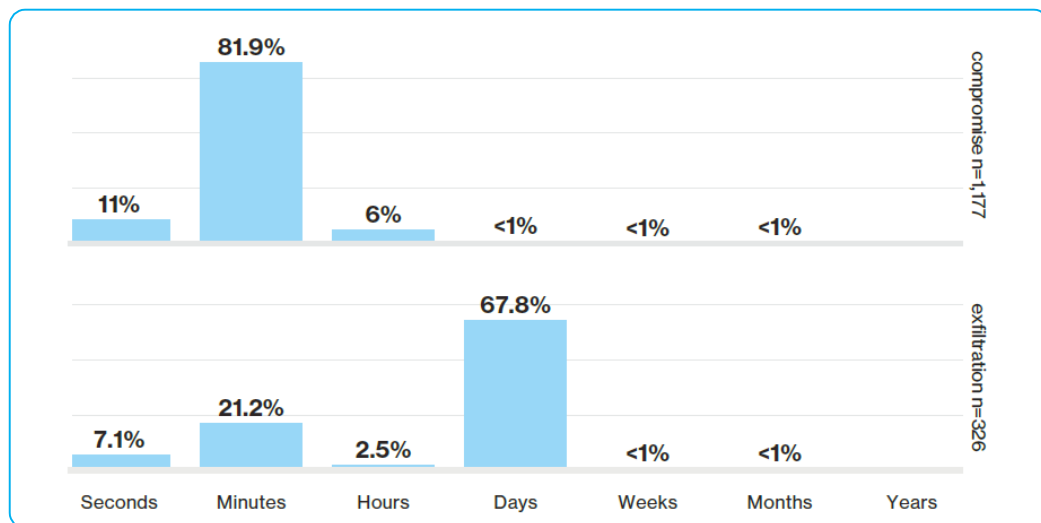
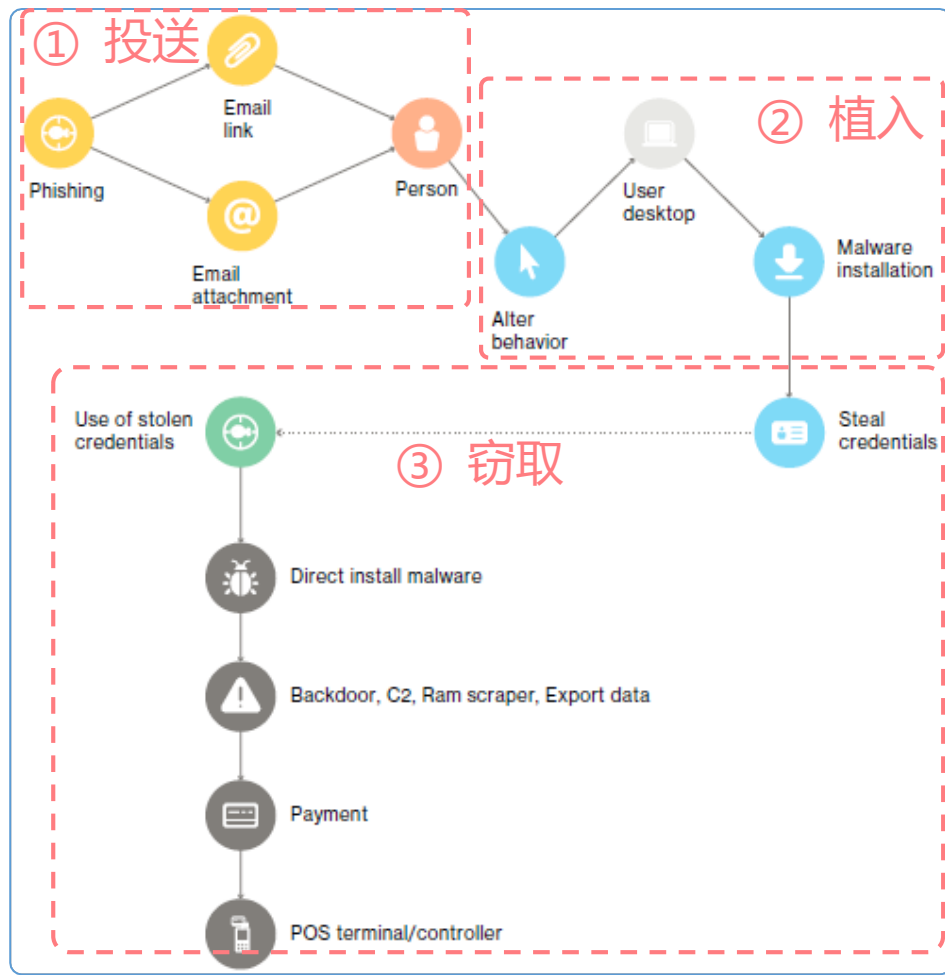


Figure 8.  
Percent of breaches where time to compromise (green)/time to discovery (blue) was days or less

- 攻入系统往往只需要几分钟时间
- 但完成数据窃取则一般需要几天

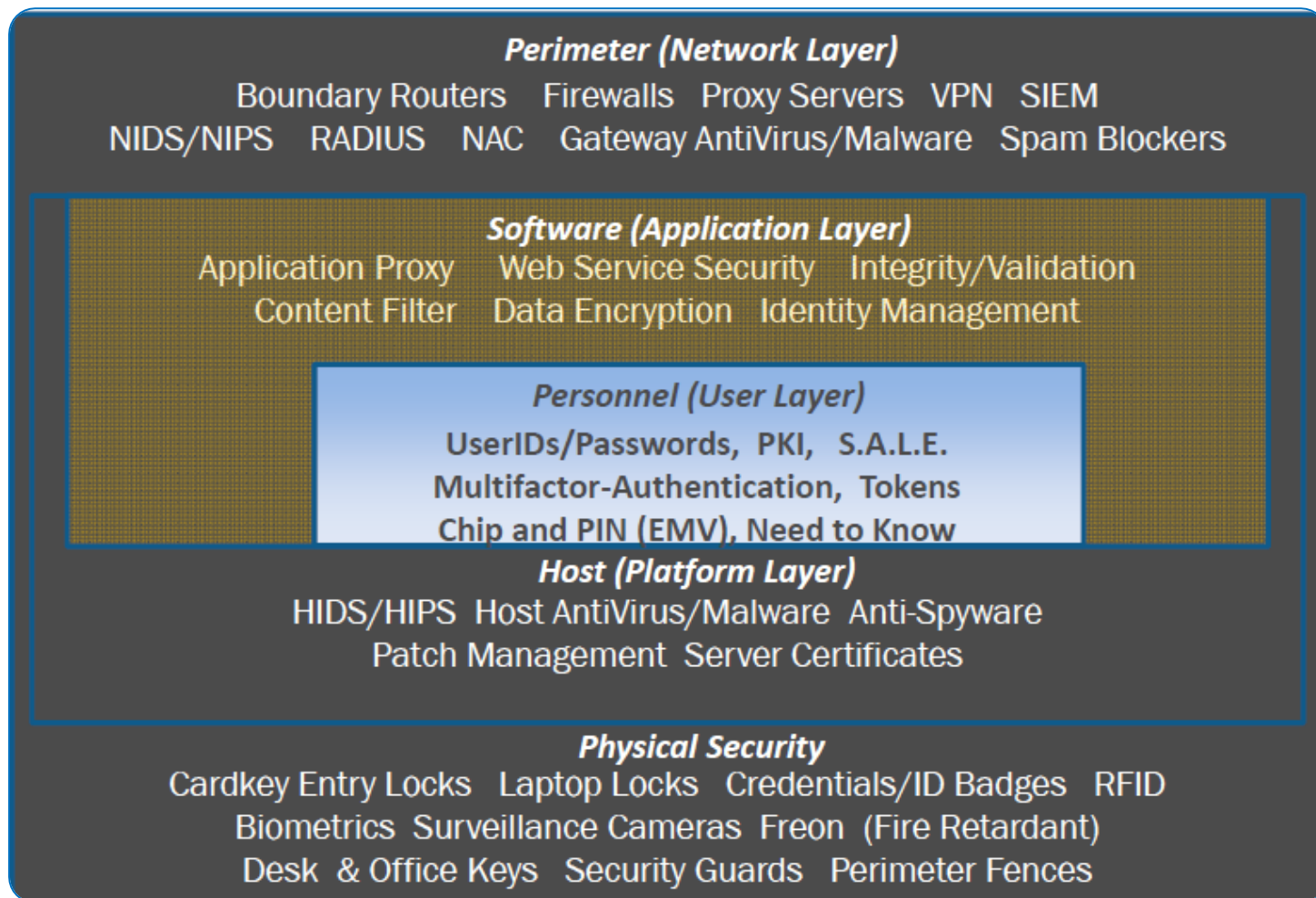
- 几天内完成攻陷的比例大幅提升
- 几天内被发现的事件未明显变化

## 数据窃取中的“关键三步”



- **Step1** : 发送网络钓鱼电子邮件，内含指向恶意网站的链接，或恶意附件；
- **Step2** : 下载恶意软件到目标PC，建立突破桥头堡，为后续针对敏感信息的进一步恶意软件植入铺路；
- **Step3** : 利用窃取的凭证进行进一步攻击，挖掘有价值的数据库。

# 数据泄漏的纵深防御体系



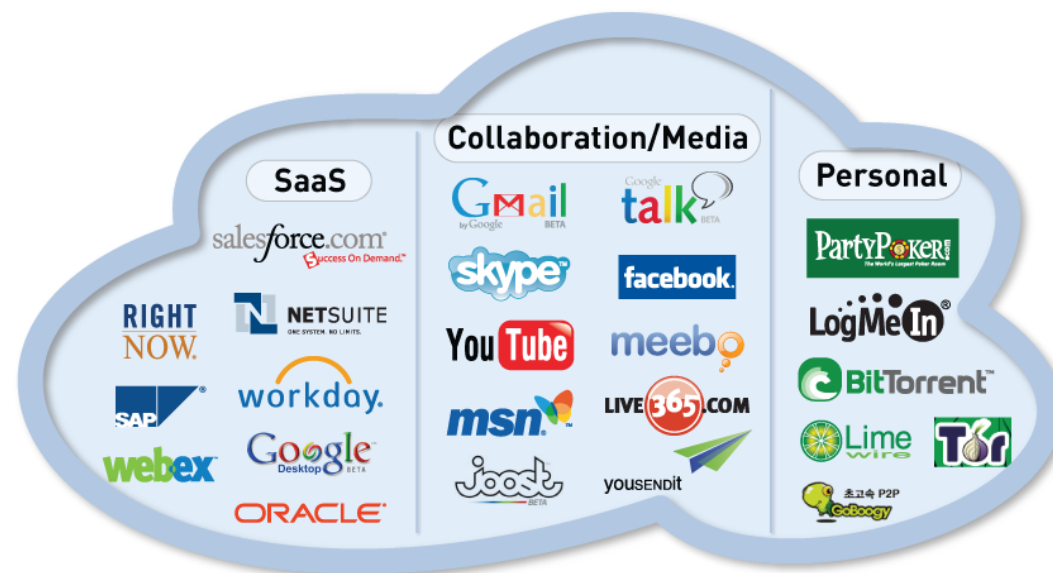
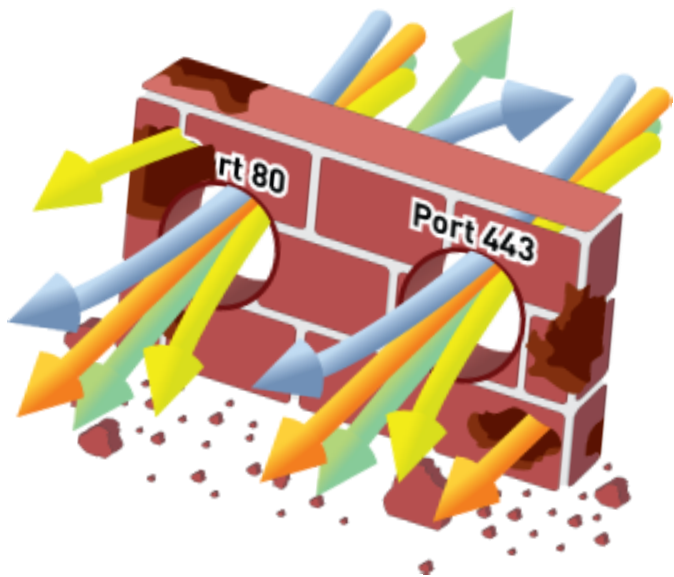
- 网络边界
- 应用系统
- 用户鉴别
- 主机终端
- 物理设施



## 网络边界是执行控制的绝佳位置，但是.....

### 机会

- 第一道也是最后一道防线
- 有机会“看到”所有流量
- 有条件执行全局主动控制



### 挑战

- 海量、不确定，真的能看清吗？
- 业务高度依赖，真的能阻断吗？
- 从“应用本身即是威胁”到“应用携带威胁”，真的安全吗？



## 网络边界防御的使命

- 应用的深度识别
- 用户和内容识别
- 应用风险视角

由可视化驱动



- 建立在可视化基础上的统一控制
- 由应用风险驱动持续的策略调优

执行精细控制



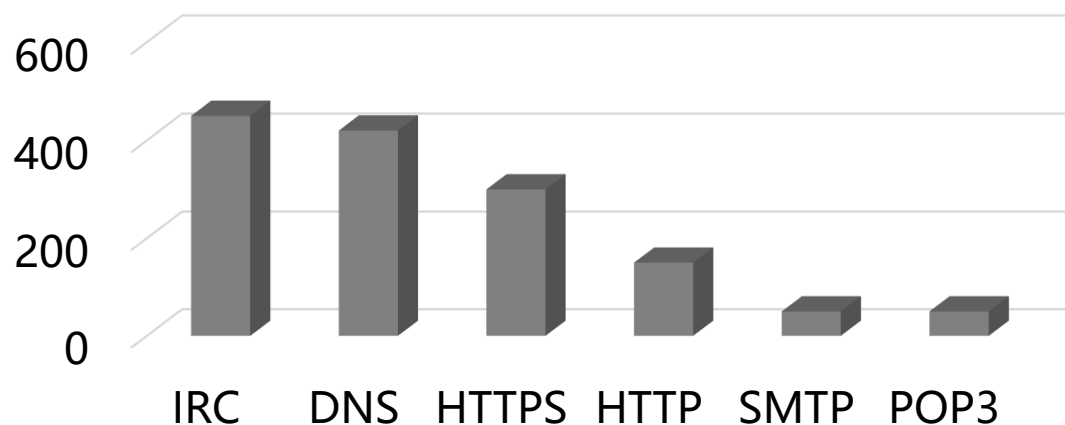
- 执行深度检查
- 引入检测、分析、感知所需的手段

面向新型威胁



# 可视化 ( Visibility ) - “看得见” 的能力

## Visualization



### • 用户能了解到的

- IRC流量最大
- DNS流量也很大

### • 用户所不知道的

- IRC属高风险应用，常被僵尸网络用于信令传输
- 最近一小时DNS流量是昨天同时间段的 300 倍

## Visibility

“可视化”不是简单的将数据图形化呈现，不是日志信息的简单分类和归集，而是深度挖掘这些原始数据素材之后的内在关联。

“可视化”提供了 **发现风险、确定风险、减缓风险** 所需的可见性，是保障边界防御有效性的基石。

### • “可视化”的关键

- 对网络流量充分认知
- 对异常情况敏锐洞察
- 对多个事件建立关联

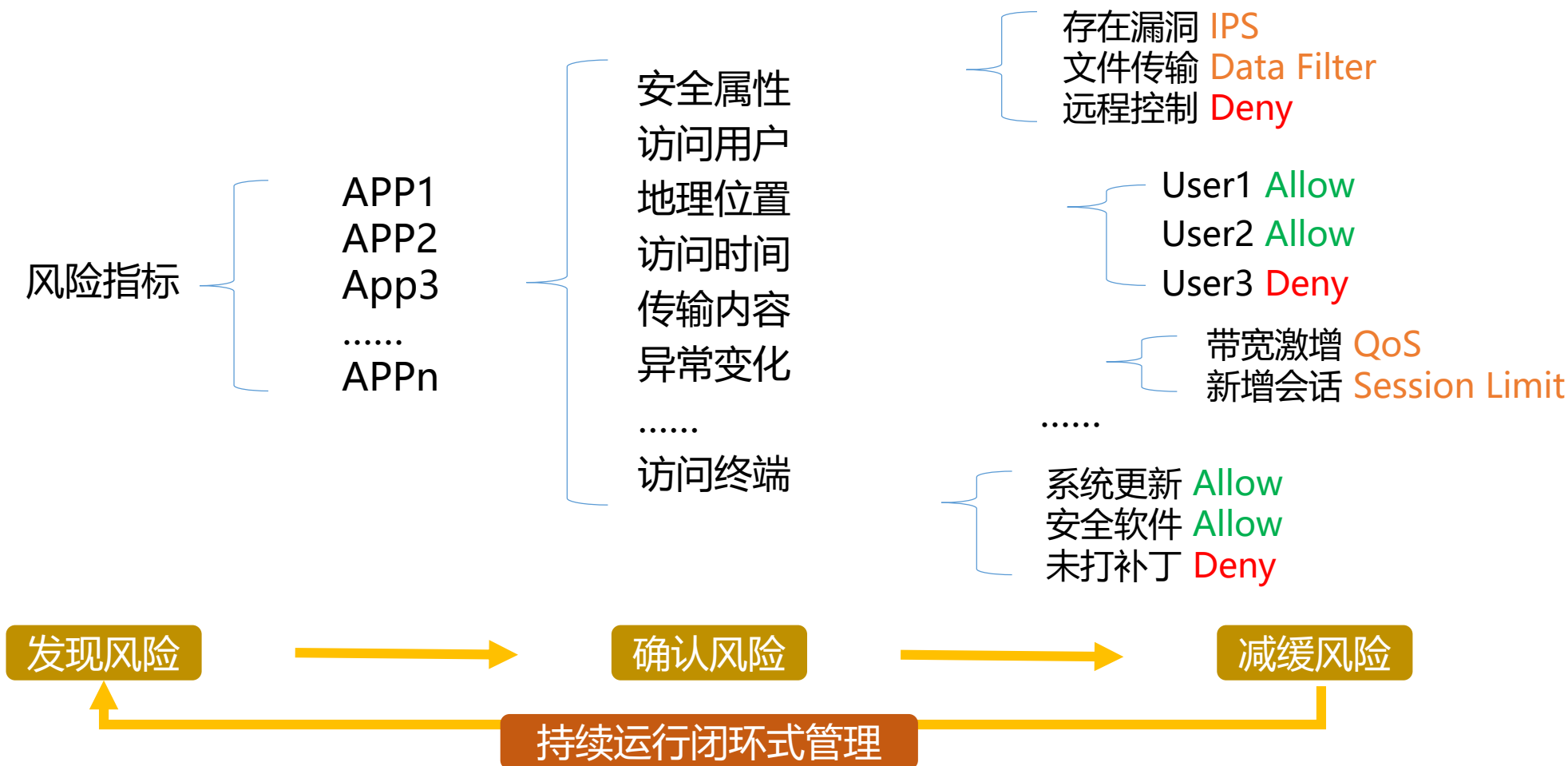
## 如何在海量应用中执行精细化控制



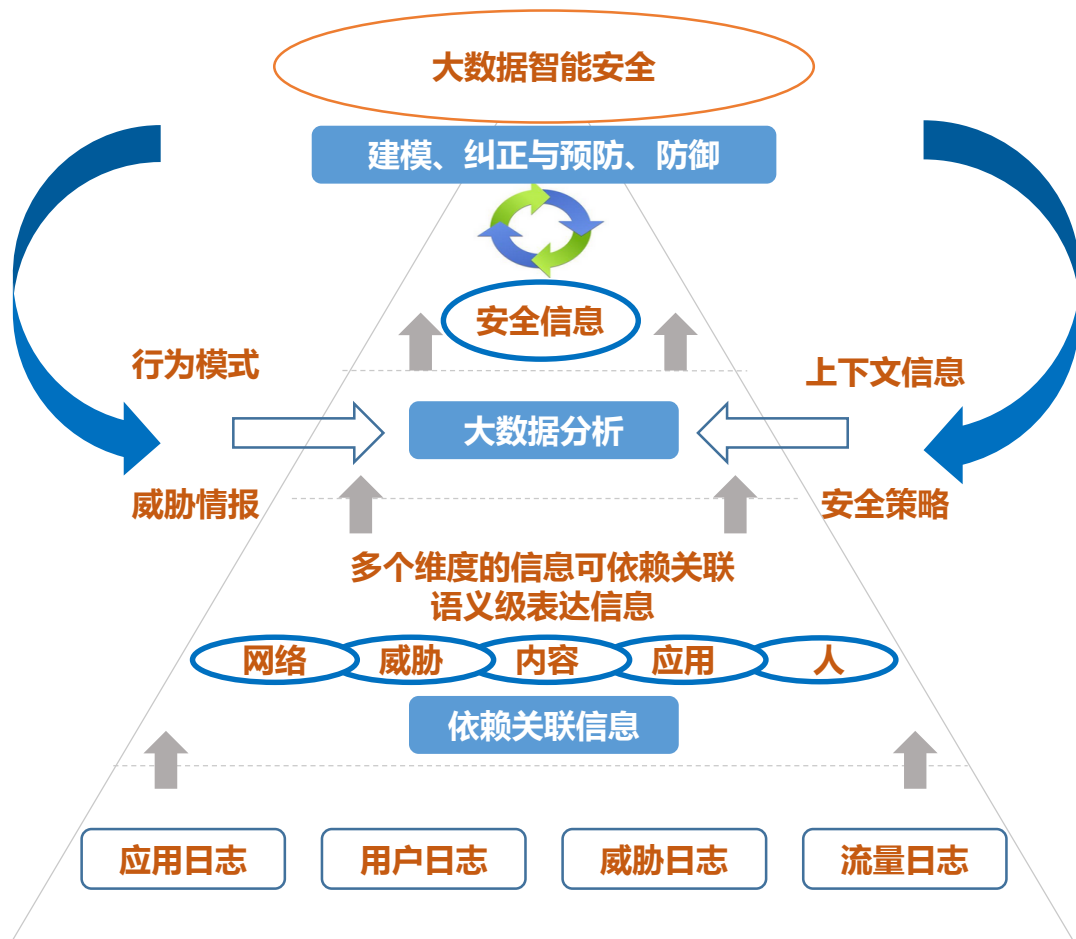
- 应用识别是边界控制的基本条件
- 业务执行所必须的应用应被放行
- 实时检测并阻断流量中携带的威胁
- 对于不确定的应用，应引入风险视角，通过持续分析决定处理方法



# 对“灰色”流量的处理



# 基于大数据进行检测、分析、溯源



C&C通信

DoS攻击

恶意扫描

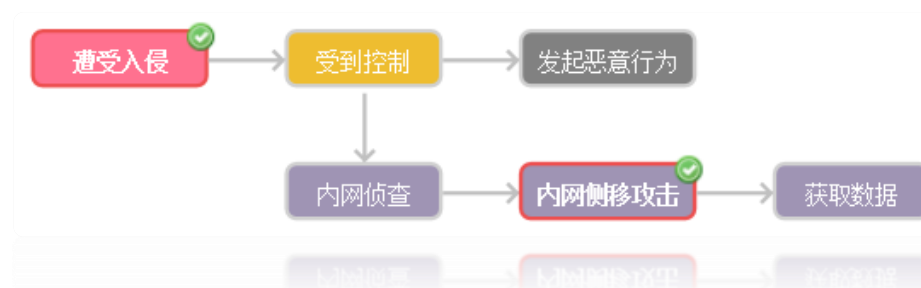
垃圾邮件

暴力破解

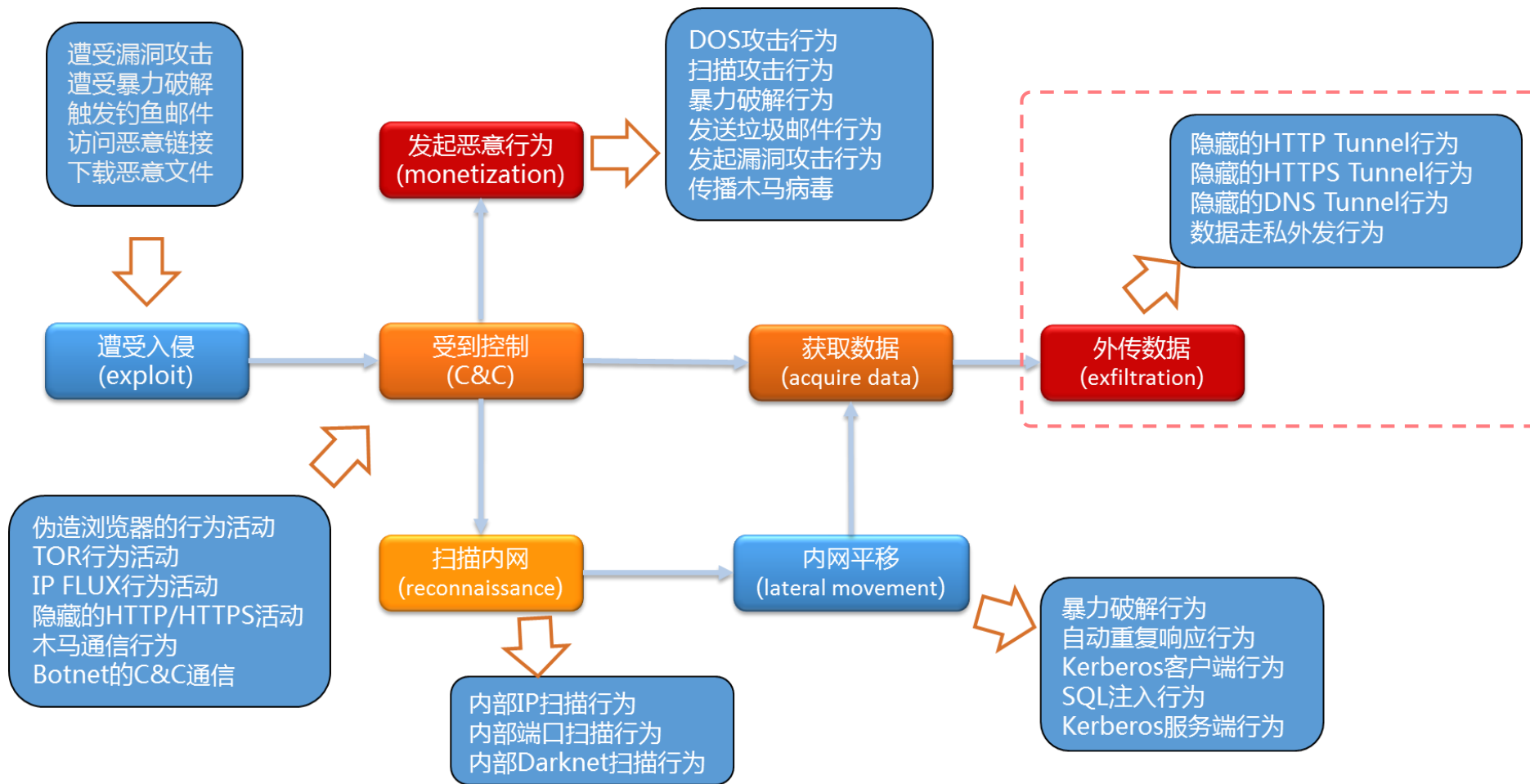
异常隧道

漏洞攻击

数据外传



# 异常行为检测 - 数据泄露的感知、预知





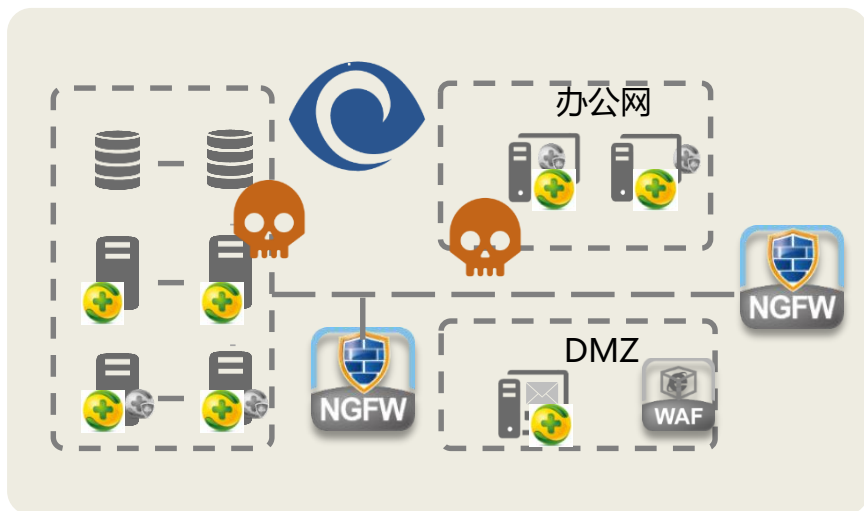
# 智能协同的边界防御解决方案

## 下一代防火墙

通过应用精细控制和深度检测，实现威胁侵入和数据泄露通道的控制

## 慧眼云

通过异常行为分析，感知、预知数据泄露风险，并提供分析溯源所需的可见性



第三方  
威胁情报

- 用户日志
- 应用日志
- 威胁日志
- 流量日志



# NGFW-可视驱动可控



数据过滤			
	文件类型	过滤类型	过滤次数
1	htm	文件过滤	5.16 K
2	swf	文件过滤	4.73 K
3	未识别	数据过滤	1.69 K
4	txt-utf-8	文件过滤	1.19 K
5	gif	文件过滤	537
6	png	文件过滤	359
7	gzip	文件过滤	283
8	html	文件过滤	174
9	htm	数据过滤	12
10	cab	文件过滤	11

安全策略			
	策略	连接数	总字节数
1	192.168.135网段	3 K	101.97 M
2	192.168.136网段	2.58 K	98.77 M
3	192.168.132网段	1.98 K	51.01 M
4	内网all	1.59 K	50.52 M
5	192.168.137网段	1.54 K	69.75 M
6	192.168.133网段	1.44 K	29.28 M
7	server192.168.101	1.34 K	80.54 M
8	192.168.134网段	1.24 K	44.8 M
9	192.168.131网段	1.18 K	61.25 M
10	All-Allow	45	608.24 K

# 慧眼云-失陷主机检测

## 当前失陷主机分布

### 主机基本信息

### 主机威胁活动详情

### 活动基本信息

活动名称 获取数据

相关主机IP 10.136.40.9

活动与确定性关系 主机感染的概率较低

活动与威胁性关系 对安全和资产威胁很小

活动解析 主机短时间内从内网其他主机获取大量数据

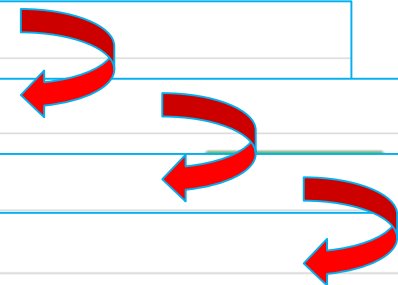
### 活动时间分布



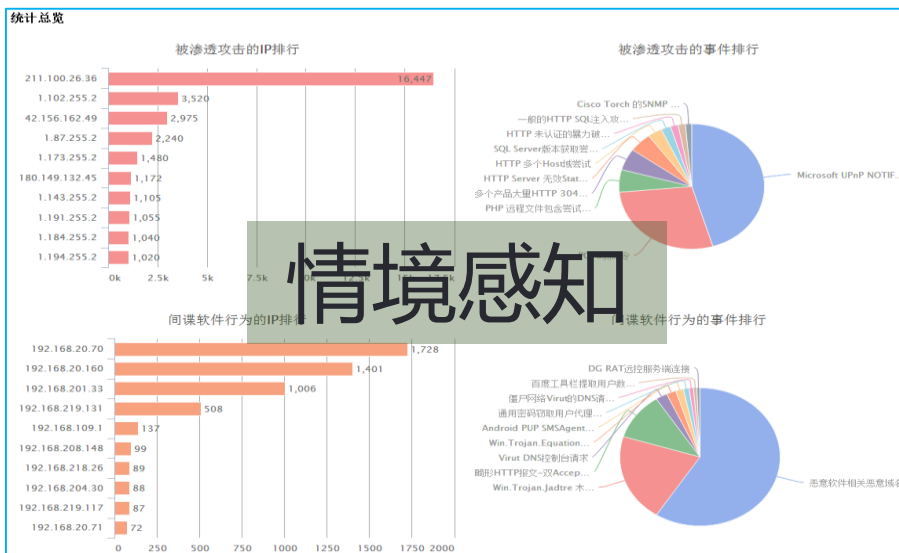
### 活动详细日志

#### 详细数据

目的地址	目的端口	开始时间	结束时间	次数	威胁名称	确定性	威胁性	数据量
10.136.40.50	1521	07-11 17:06:43	07-11 17:06:43	1	● 获取数据	40 <a href="#">✎</a>	30 <a href="#">✎</a>	130MB







# 小结



**Prevention** : 执行精细化访问控制，收缩威胁入口和泄露通道

**Detection** : 进行多维的行为检测，及时发现失陷和泄漏风险

**Response** : 关联分析、高效回溯，为响应措施提供决策依据



2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT

谢谢！