2017 中国互联网安全大会
China Internet Security Conference

网络空间安全新尺度

张晓兵 途隆云 CEO

网络的尺度

Network 网络/IT	Internet 互联网/NT	CyberSpace 网络空间/DT
□ 局域网 □ 城域网 □ 广域网	□ PC互联网 □ 移动互联网	□ 云计算/大数据 □ 万物互联（IOT） □ 互联网+

- **业务前移是必然趋势！**

安全的“暗物质”

勒索病毒

2017年5月12日，WannaCry“永恒之蓝”勒索蠕虫爆发，攻击了近百个国家的近4万家企业，在中国有上百万台服务器中招，中招者要限时支付价值300美元的比特币才能解锁，否则销毁数据。

无敌舰队

2017年6月15日起，“无敌舰队”组织向国内多家证券金融公司、互联网金融公司发起DDoS比特币勒索，现已有超过6家金融证券类企业遭受DDoS攻击勒索，且其中4家已经遭受了大规模的DDoS攻击。

安全理论的尺度

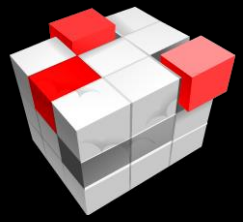
P2DR模型

安全运维尺度

木桶理论

产品尺度

立体防御

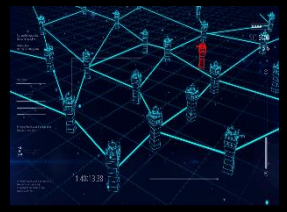


系统尺度

云管端

网络尺度

安全塔防

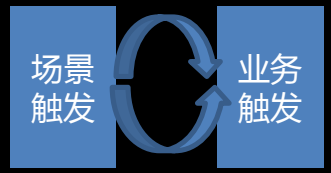


协同与联动尺度

自适应安全

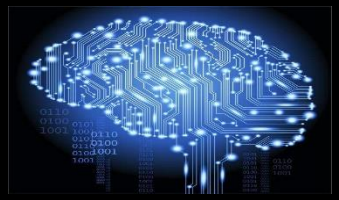
云计算尺度

主动安全



业务尺度

智能安全

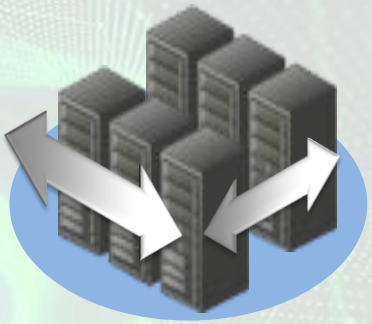


人的尺度

Network → Intranet/Internet → Cyber Space

安全的发展尺度

1990 2015

终端安全	网关安全	网络空间安全	大数据安全
			
边界防御思想（木桶理论）		资源与数据驱动思想（协同）	
单点防御—立体防御	P2DR—云管端—安全塔防	单点防御--云防护—单点抗D	威胁情报—态势感知—人工智能

安全的未来尺度

01

安全是药

- 单机防护体系
- 被动点式防御

静态安全

02

安全是保险

- 合规安全体系
- 被动线式防御

塔防体系

03

安全是健康

- 业务驱动体系
- 主动式防御

主动安全

未来网络空间安全的四大基础能力

安全态势感知能力

发现

网络攻击防御能力

防御

漏洞发现防御能力

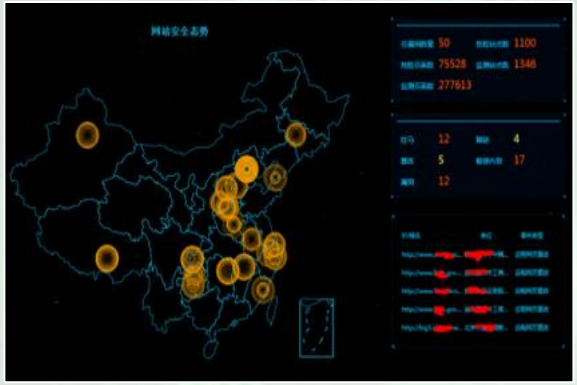
加固

数据安全保障能力

保障

安全看见能力的尺度：态势感知

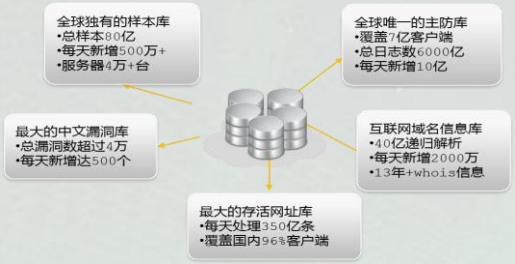
- **企业现状：态势感知是安全建设的最后一环**
- **解决安全的哲学命题：你是谁？你从哪里来？你要到哪里去？**

安恒态势感知	绿盟态势感知	360态势感知
		

- **态势感知不单单是可视化与溯源**

态势感知的尺度

威胁情报



- 收集多维度安全数据
- 探知多维度的安全点

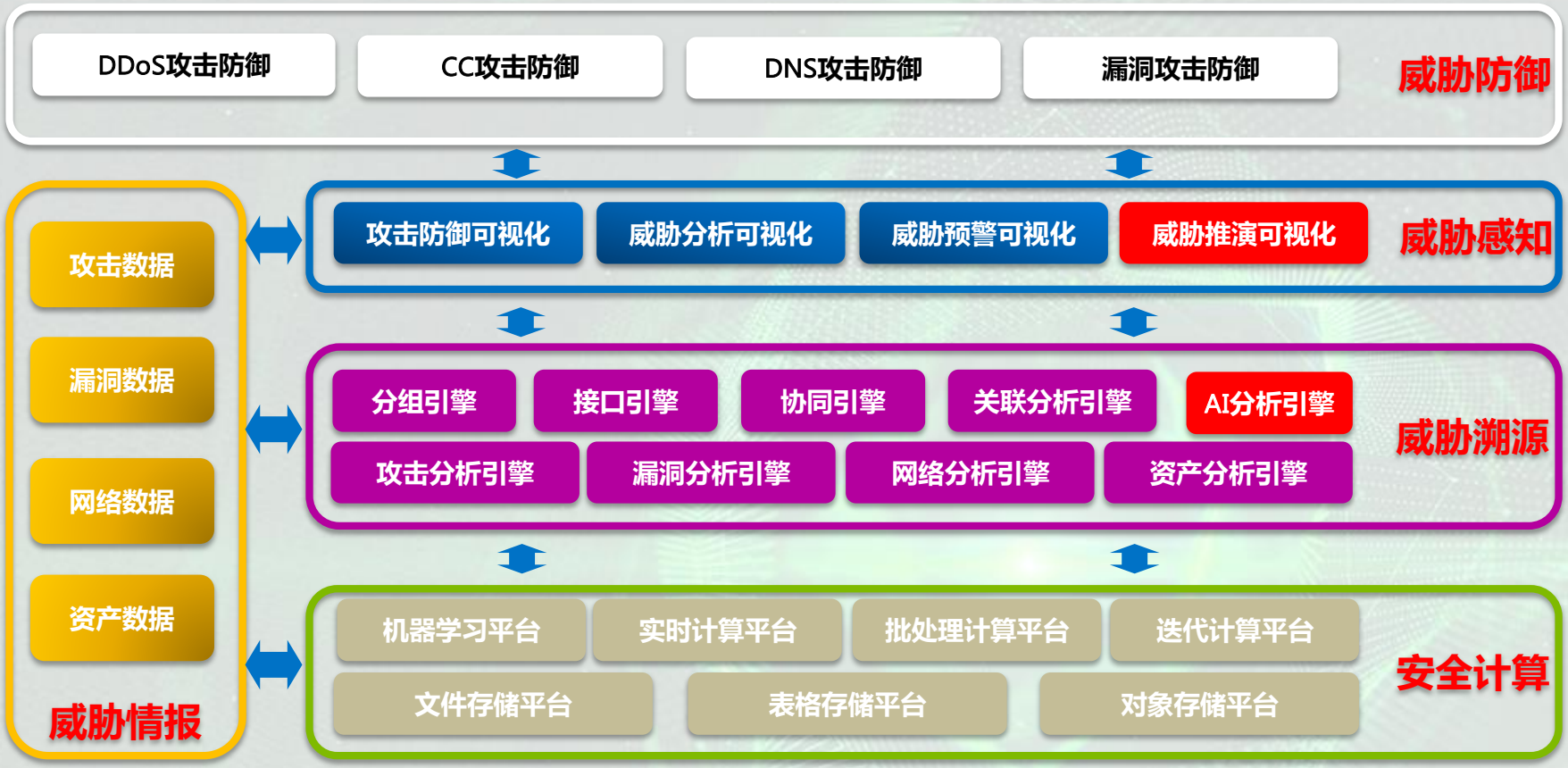
威胁感知

- 安全可视化
- 攻击者画像

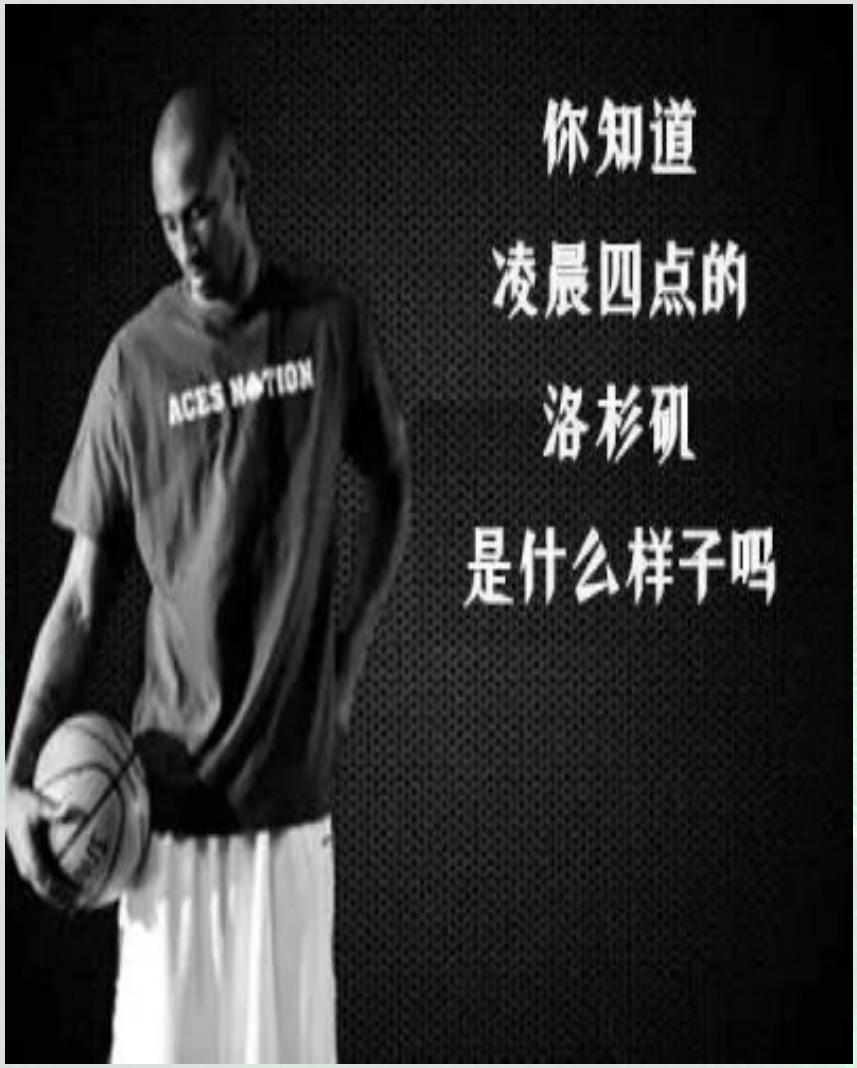
攻击溯源

- 攻击关联分析
- 攻击溯源
- 攻击感知

途隆云的态势感知尺度


DDoS攻击防御
CC攻击防御
DNS攻击防御
漏洞攻击防御
威胁防御
攻击防御可视化
威胁分析可视化
威胁预警可视化
威胁推演可视化
威胁感知
攻击数据
漏洞数据
网络数据
资产数据
威胁情报
分组引擎
接口引擎
协同引擎
关联分析引擎
AI分析引擎
攻击分析引擎
漏洞分析引擎
网络分析引擎
资产分析引擎
威胁溯源
机器学习平台
实时计算平台
批处理计算平台
迭代计算平台
文件存储平台
表格存储平台
对象存储平台
安全计算

网络攻击的尺度



阿里云盾：

2016年《2015年下半年云盾互联网DDoS状态和趋势报告》数据：

- 2014 年云盾遭遇最大的DDoS攻击峰值为 453.8Gbps 。
- 2015 年云盾遭遇最大的DDoS攻击峰值为 477Gbps 。

百度安全：

2017年3月发布的《 2016年DDoS攻击报告》数据：

- 2016年最高峰值达到 385G

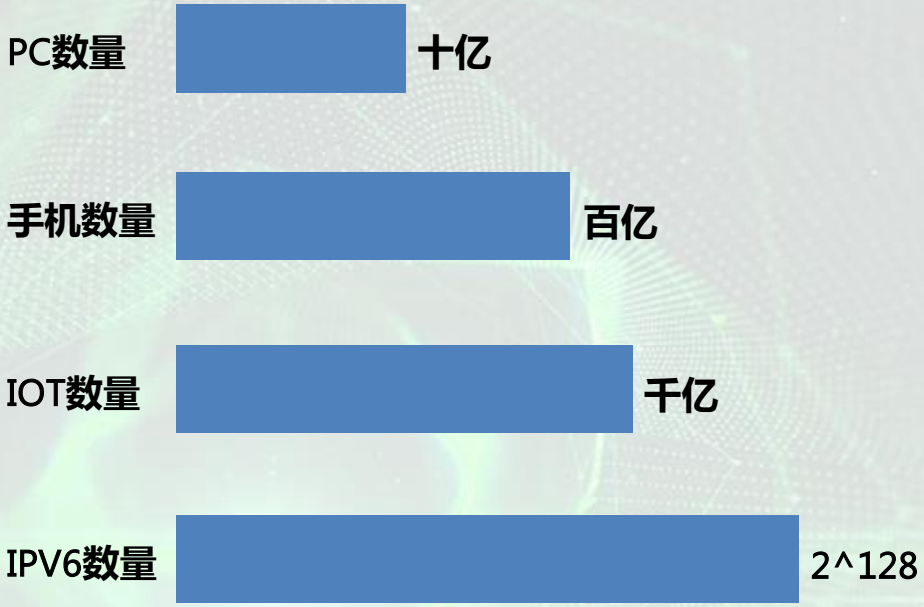
途隆云：

- 2017年4月，为某游戏客户抵御近800Gbps的攻击
- 2017年5月， 遭遇黑客组织公开挑战，成功抵御650Gbps攻击
- 2017年6月，遭到"暗云III" 攻击，最大901Gbps攻击,在持续10小时攻击过程中，累积防护攻击量达63Tbps。

网络攻击的未来尺度

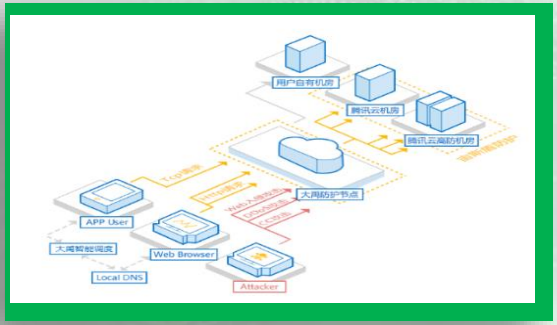
2017：CloudFlare presentation to Security Working Group

年限	攻击载体	攻击峰值	攻击类型	防御手段
2012年	IDC僵尸主机	30~50Gbps	SYN Flood	Anti-DDoS硬件设备
2014年	PC僵尸 IDC僵尸主机	100G 常态化	反射型UDP flood	IDC高防机房
2016年	PC僵尸 IDC僵尸主机 IoT 移动终端	200G 常态化	真实设备流量型攻击，CC攻击	公有云高防服务方案
2017年	PC僵尸 IDC僵尸主机 IoT 移动终端	1T攻击时有发生	模拟私有协议的真实设备流量攻击（CFA）	带调度平台的公有云高防服务方案
将来	PC僵尸 IDC僵尸主机 IoT 移动终端	1T攻击常态化	以上攻击类型总和	基于运营商近源清洗的公有云高防服务方案



- 2016年，美国东海岸断网： 1000万物联网设备

途隆云：网络攻击防御的新尺度

1.0 **设备抗D**	2.0 云防护	3.0 **单点抗D**
		
	• **IP轮询/IP扫段**	• **单机房 BGP线路防御能力达2.3T**

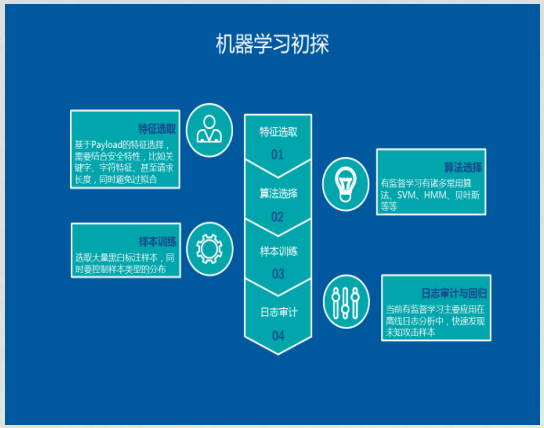
智能安全尺度：AI与人

AI1.0 封闭域	AI2.0 开放域	AI3.0 **安全域？**
机器学习：有限数据集中的模式匹配 • **指纹** • **人脸** • **OCR**	**深度学习：无限数据集中的深度搜索与评价** • **博弈** • **自动驾驶(二维有序量)** • **声音识别（一维有序量）**	一维无序量中的模式识别 • 样本识别 • 流量识别 • 攻击行为识别

- **AI倒底是代替人类还是超越人类？**
- **智能VS智力？**
- **AI在安全里能够起到什么作用？**

AI的人的尺度：安全厂商在用AI做什么？

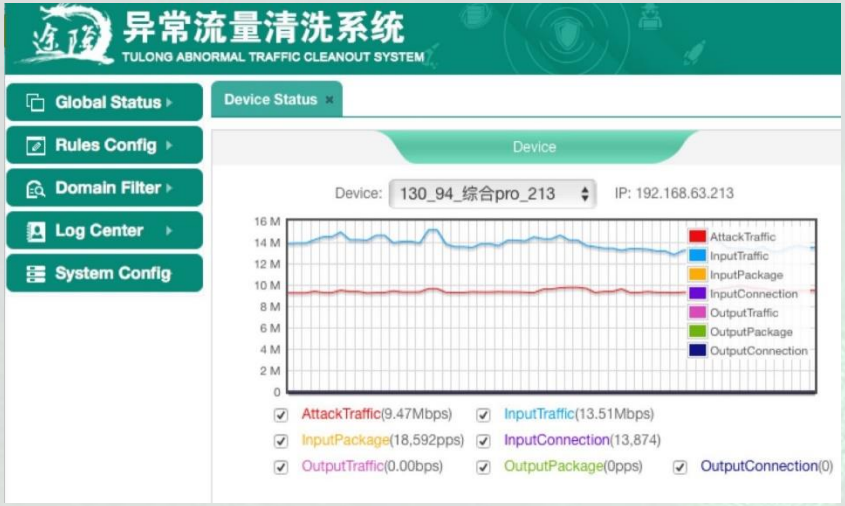
百度安全：WEB安全检测

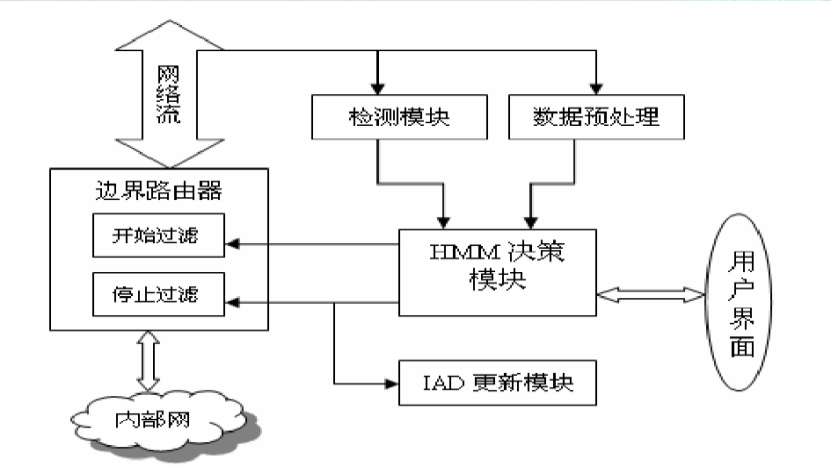


腾讯云：AI安全矩阵

- **用AI来做威胁预测是个伪命题**
- **AI可以代替人类活动中的重复劳动部分**

途隆云的AI尺度





方法：

- 根据正常数据流进行常用 IP 地址库的学习，使常用 IP 地址库中保存常用的源 IP地址信息
- 然后进行模型参数的学习，使隐马尔可夫模型准确的描述网络数据流的动态 IP 地址序列
- 离线学习完成后，基于 HMM 的 DDoS 检测系统进行实时检测
- 同时，IP 地址库在线学习机制保证 IP 地址库的准确性和有效性

应用：

- DDoS攻击的识别
- 攻击小组攻击工具的识别

谢　谢

ISC 2017
中国互联网安全大会

360互联网安全中心