

## 互联网时代下的企业安全变革

——网康科技CEO袁沈钢





### 安全市场将出现井喷式增长

#### 中国安全市场预测(亿美元)

■2014中国IT市场规**信息安全搜**免全**店**标授入 比重2018年中国安全市场规模



■信息安全投入占Ⅱ投入比重



### 众多新技术将安全带入下一代

代表企业: CloudFlare

安全云 技术

代表企业: Splunk

大数据 技术

下一代 安全

代表企业: Paloalto

应用层 技术

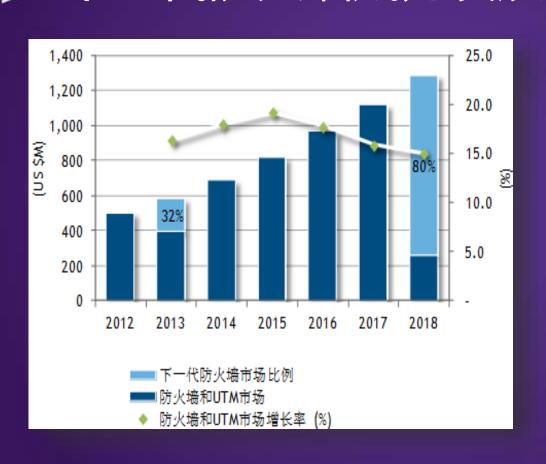
代表企业: FirEye

沙盒技术

白名单 技术 代表企业: bit9



### 下一代防火墙成为发展方向



预计从2013到2018

年,下一代防火墙占总体防

火墙和UTM市场的比例将从

30%上升到<mark>80%,5</mark>年复合增

长率超过40%。

IDC《下一代防火墙白皮书》



### 防火墙的发展

第一代:包过滤防火墙

第三代:应用 代理防火墙

第五代: 自适应代理防火墙

第七代:下一 代防火墙

第二代:电路层防火墙

第四代:状态 检测防火墙

第六代:统一 威胁管理

#### 1994年, CheckPoint

- 基于IP、端口的访问控制
- 检查数据包头的异常特征
- 较强的三、四层转发能力

#### 2004年, IDC

- 基于IP、端口的访问控制
- 检查数据包头及载荷部分
- 串行架构,全开启性能衰减率约90%
- 安全数据割裂分散

#### 2009年, Gartner

- 基于应用特征的访问控制
- 检查数据包头及载荷部分
- 一体化架构,全开启性能 衰减率约50%
- 安全数据整体关联

第四代:状态检测防火墙

第六代:统一威胁管理

第七代:下一代防火墙

- 禁止越权访问以及非法连接的建立是防火墙的核心目标和基本功能
- 防火墙技术的历次升级是为了在新的安全背景下更好的实现其功能



### 防火墙的进化逻辑

### 始终通过三大能力的增强提升用户的安全性

### 数据通信

• 网关产品的必要条件

#### 访问控制

• 防火墙的最核心目标

#### 特征匹配

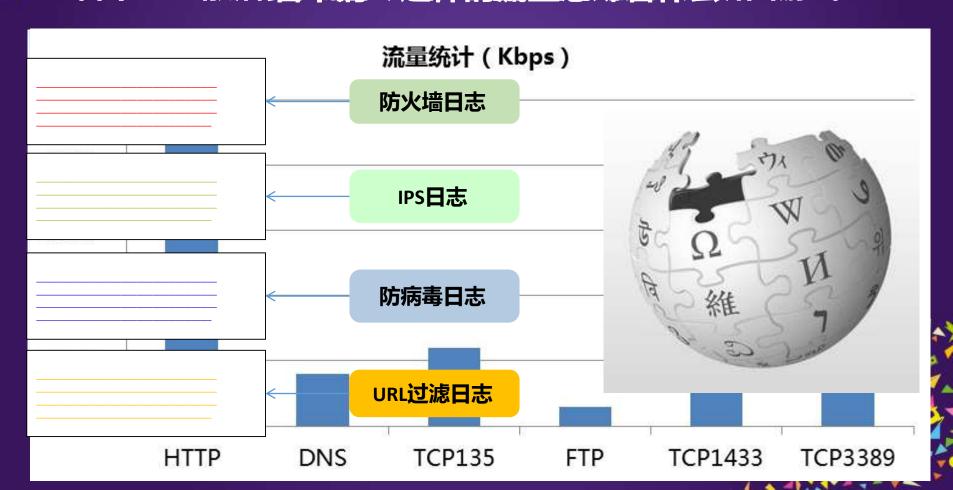
• 为了更好的访问控制

- NGFW的能力体现
  - 数据通信:较高的性能、IPv6、虚拟防火墙等
  - 访问控制:由元组控制提升为人、应用、内容控制
  - 特征匹配:病毒、木马等应用层威胁的识别和防御



### 河察力:被忽略的第四大能力

看不全:散落看來情安全样的機劃等機屬地如拼图游戏





## MGFW 的全网洞察力

図康i NETEN	科技 ITSEC 英独映版	空田分程 粉括中で	、 全敗死學 用白苧油 网络	现 <del>里</del> 安公等田			₩ 保存
详情							×
常规				源		目的	
会话ID:	2151411542	威胁类型:	防病毒	源用户:	10.198.20.100	目的用户:	未定义账号
时间:	2014-04-09 15:42:52	威胁名称:	HEUR/Malware.QVM11.Gen	源IP:	10.198.20.100	目的IP:	42.121.254.142
应用:	二进制文件下载	威胁分类/	9.rar	源端口:	52967	目的端口:	80
IP协议:	TCP	内容:		源国家:	10.0.0.0-10.255.255.25	目的国家:	中国
策略:	允许	严重性:	严重	源区域:		目的区域:	
动作:	阻断						
			事件	溯源			
				<	>		
关联日志							
时间	日志	类型 应用	劫作 策略	总字节数	包数 严重性 分类	URL/文件名	

时间	日志	类型	应用	劫作	策略	总字节数	包数	严重性	分类	URL/文件名
2014-04-09 15:42:45	网址过滤		二进制文	允许	允许				网络资源	files.cnblogs.com/cfdown/9.rar
2014-04-09 15:42:45	数据过滤	文件过滤	二进制文	告警	允许				осх	9.rar
2014-04-09 15:42:52	威胁	防病毒	二进制文	阻断	允许			严重	9.rar	
2014-04-09 15:43:32	流里	连接结束	二进制文	允许	允许	68542	86			



### 了互联网精神的核心在于用户体验



### 用户体验是唯一标准

- 只有价值需求没有合规需求
- 只有客户有权利评价一款产品
- 从客户体验到公司的业绩的传导基本没有误差
- 必须关注客户体验,只需关注客户体验!

### 口碑的力量超越广告

- 口碑营销, 粉丝营销是互联网时代的产物
- •一个满意的客户会带来100个新客户, 反之亦然
- 企业将重点重新回归到为人民服务上来



### 至耳联网化的产品设计更注重用户参与

及时呈现配置 调整后的效果 并进一步优化

## 检测 效果



呈现网络的流 量、威胁、风 险及安全事件



快速 响应



提出建议

用数据为安全 策略的调整给 出建议





### 少以互联网精神决胜企业级市场

强大的用 户粘性

- 强调交互
- 及时反馈

使他爱用 互联网化的 下一代安全

极致的操 作体验

- 大众参与
- 简单易用

帮他会用

下一代安全

用户需求 为导向

- 技术创新
- 解决问题

对他有用

传统安全



# THANK U!

