



2016 中国互联网安全大会
China Internet Security Conference

协同联动 共建安全+命运共同体

云端威胁的智能化监测与防护

孙震

Ixia China
应用和安全业务发展总监

AGENDA

- 全网络流量可视化和分析
- 基于云端的恶意IP拦截技术
- LAB环境里再现真实世界流量



中国互联网安全大会



360互联网安全中心

全网络流量可视化和分析

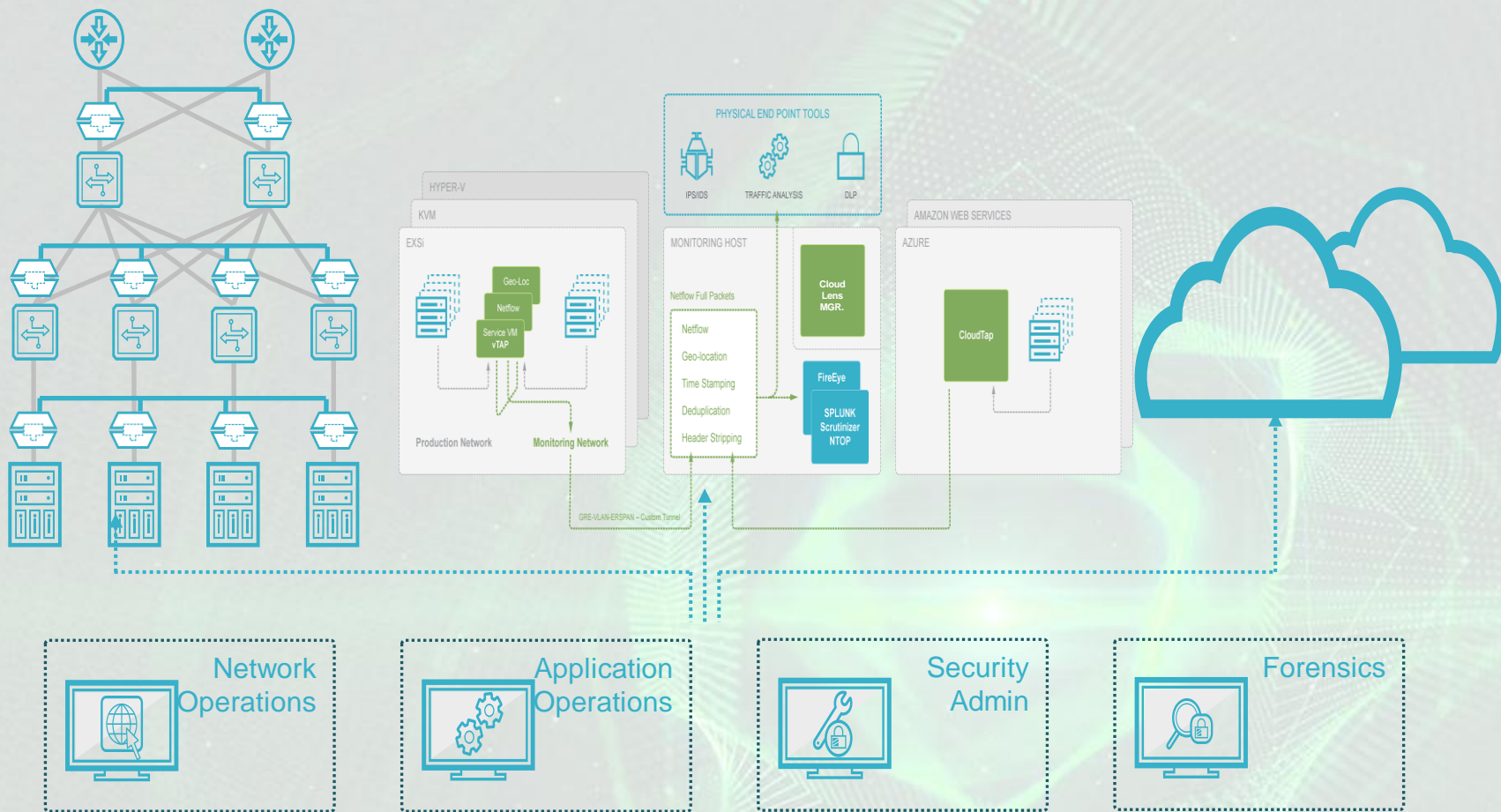
企业网全环境可视化系统



中国互联网安全大会



360互联网安全中心



Vision : 一个平台完成物理 / 虚拟 / 云 全环境的流量可视化和智能监测

全环境可视化的统一实时流量分析系统 - ATIP



中国互联安全大会



360互联网安全中心

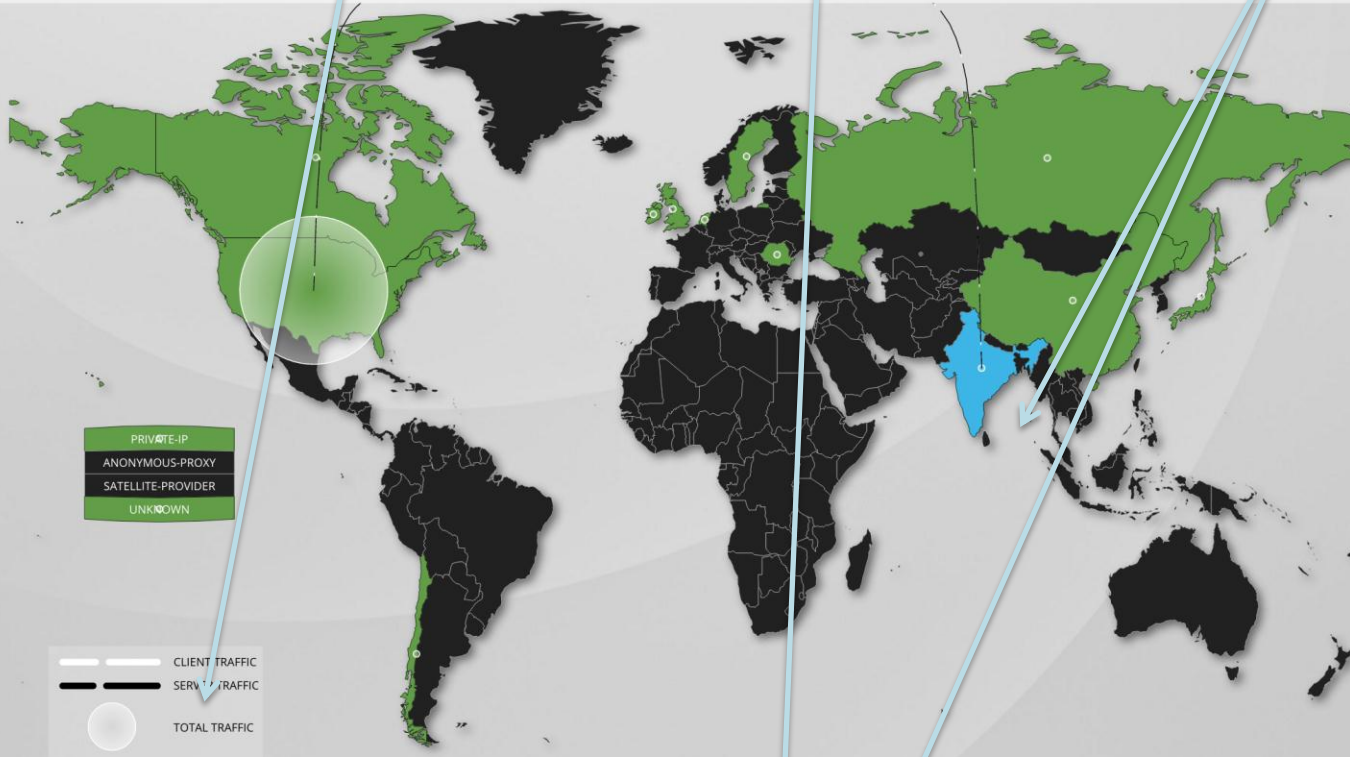
精细化追踪

特定信息的详细深入分析

IP地址归宿分类 / 记录

各层次数据统计

WORLD (LAST HOUR)



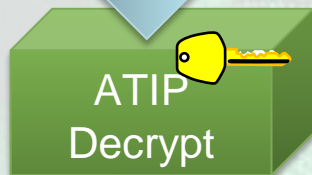
TOP GEOS (SESSIONS)

Country	Sessions	Server Pkts	Client Pkts	Server Bytes	Client Bytes
Private-IP	1,996	11,876	16,592	11.2 MB	2.3 MB
Unknown	19,523	648	6,812	59.3 KB	1.3 MB
Canada	41	1,070	0	1.1 MB	0 bytes
Ireland	14	844	0	904.9 KB	0 bytes
Romania	160	0	1,524	0 bytes	69.2 KB
United Kingdom	62	65	4	7.8 KB	392 bytes
Europe	1	27	0	6.7 KB	0 bytes
India	4	0	21	0 bytes	973 bytes

TOP APPS (LAST HOUR)

App	Sessions	Total P...	Client ...	Server ...	Total B...	Client ...	Server ...	Sha... ↓
SIP VoIP	20	9,015,239	9,015,239	0	12.3 GB	12.3 GB	0 bytes	82%
microsoft-ds (TCP:445)	2,639	836,816	836,816	0	971.8 MB	971.8 MB	0 bytes	6%
ixiacom.com	19	494,290	494,290	0	682 MB	682 MB	0 bytes	4%
10.218.200.107	12	431,385	431,385	0	621.3 MB	621.3 MB	0 bytes	4%
IMAP	1	229,242	229,242	0	158 MB	158 MB	0 bytes	1%
https (TCP:443)	3,852	160,727	160,727	0	124.8 MB	124.8 MB	0 bytes	1%
10.218.201.6	14	63,896	63,896	0	91.1 MB	91.1 MB	0 bytes	1%
ssh (TCP:22)	108	31,268	31,268	0	33.7 MB	33.7 MB	0 bytes	0%

问题1:分析加密数据



Clean

搜索 / 查找



归类 / 存储



问题2:用户隐私保护



中国互联网安全大会



360互联网安全中心

Source Data

SSN: 123-45-6789
Credit Card: 1234 567890
12345
Name: John Smith
Birthday: 03/19/1963

ATIP Data

SSN: XXX-XX-XXXX
Credit Card: XXXX XXXXXX
XXXXX
Name: XXXX XXXXX
Birthday: XX/XX/XXXX

DATA Masking



中国互联网安全大会



360互联网安全中心

基于云端的恶意IP拦截技术

“企业每年 21,000 小时被用于处理误报的安全报警”

Ponemon Institute , 2015 年



每个网络上都有两类流量

值得分析：
可能有价值的流量

不值得分析：
已知恶意软件网站

被劫持IP

未登记的IPs

无关的地区



在现有安全架构上部署ThreatArmor减少受攻击面







中国互联网安全大会



360互联网安全中心



 未注册的IP
 被劫持的IP

 已知Malicious IP
 无关地区的IP

基于云的恶意IP监控系统



中国互联网安全大会



360互联网安全中心



Tracking
IP addresses

恶意IP识别与处理流程



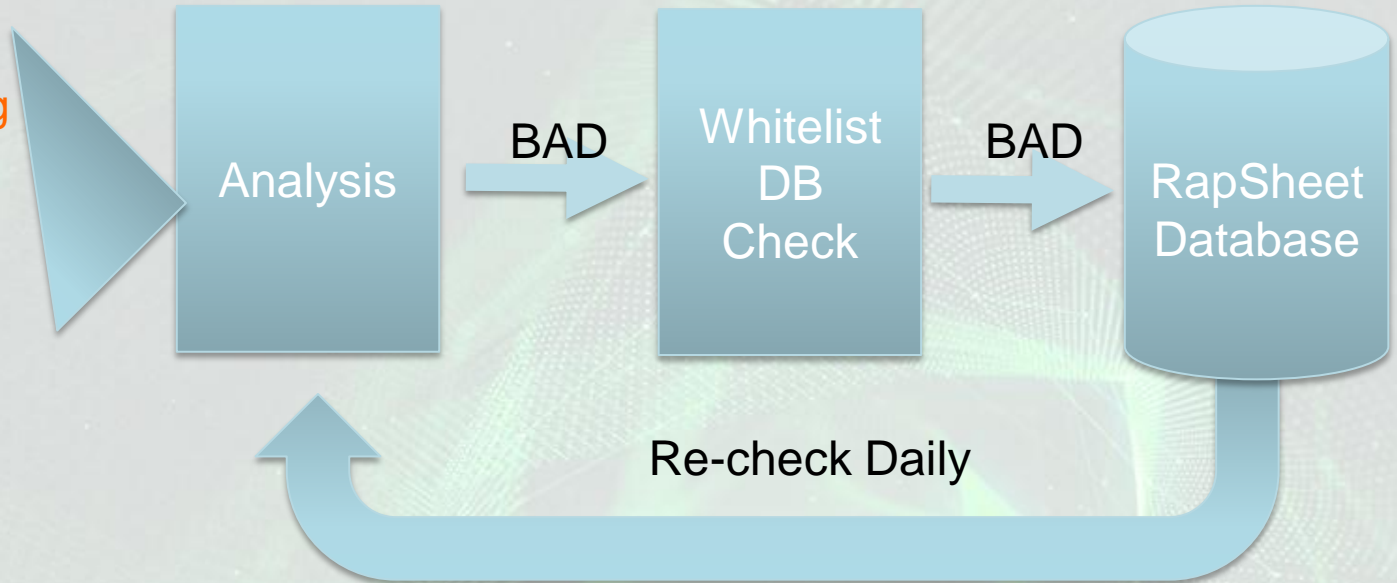
中国互联网安全大会



360互联网安全中心

1. Source Feeds
2. Internet Scanning
3. Honeypots
4. SPAM
5. Binaries
6. Sandboxes

.....



Analysis Engine

AV
Detection

Sandbox
Execution

Phishing
Engine

Ixia
Signatures

数据来源和处理



中国互联网安全大会



360互联网安全中心

- **Source Feeds**
开源，付费，合作

—————>

进入系统前会逐个进行再验证和确认
- **Internet Scanning**
7×24小时识别病毒和漏洞

—————>

7×24小时扫描，病毒网站直接入库，有漏洞网站进入特殊序列以做再扫描
- **Honeypots**
SSH, FTP, RDP, VoIP, HTTP等服务

—————>

全球部署，ixia定制蜜罐，记录试图连接者，以做进一步检查
- **SPAM**
内部收集，付费信息...

—————>

钓鱼网站探测，自学习引擎，人工确认
- **Binaries Analysis**
已知malware，第三方APP Stores...

—————>

确认一个Site是否有恶意行为的最后关键一步；AV引擎，静态对比，机器学习，沙箱 ...
- **Sandboxes**
Malware意图连接目的地址检查...

—————>

带有ixia特征库的沙箱

恶意IP确认机制



中国互联网安全大会



360互联网安全中心

1. 100% 确认
2. 完整清晰的证据
3. 以行为为依据，不做道德等其它判断
4. 周期性复查
5. 被修复IP从库移除，但被永久保存监控

.....

白名单机制



中国互联网安全大会



- Alexa/Quantcast 排名前10,000的网站
如: Facebook, Google, YouTube, etc.
- 云服务提供商:
如 : Amazon AWS, Microsoft Azure, Salesforce, etc.
- 关键的互联网基础设施 :
如 : Root DNS servers, NTP servers, etc.
- 企业的IT应用 (来自于客户) :
如 : Office 365, AV/OS update, CDN,

IP:185.61.100.100 IP:202.97.100.100 IP:95.173.100.100 IP:221.14.100.100 IP:205.20.100.100 IP:5.196.197.221

RAP SHEET | RAP SHEET | LI | RAP SHEET | LO | RAP SHEET | LC | RAP SHEET | LC | RAP SHEET | LOCAL IP ADDRESSES

THREATS DETECTED: 1 PHISHING, 1 MALWARE

JS:IFRAME

THREAT URL

LAST SCAN DATE
FILE CHECKSUM

PAGE TITLE



JS:IFRAME

THREAT URL

LAST SCAN DATE
FILE CHECKSUM

COMMUNIST WIN32/TROJAN

LAST SCAN DATE
FILE CHECKSUM

COMMUNIST WIN32/TROJAN

LAST SCAN DATE
FILE CHECKSUM

HTML/PHISHING

THREAT URL

LAST SCAN DATE
FILE CHECKSUM

PAGE TITLE



HTML/PHISHING

THREAT URL

LAST SCAN DATE
FILE CHECKSUM

PAGE TITLE

PERFORMANCE

LAST SCAN DATE

HIJACKED

This particular IP address is used for any number of purposes. For example, it is used for http://www.sj.com/

LAST SCAN DATE
MORE INFO AVAILABLE

ASN
ASN REGISTRATION
ASN DESCRIPTION
ASN REGISTRATION DATE
ASN (AUTONOMOUS SYSTEM NUMBER)

PHISHING PAGE

THREAT URL

<http://mhp-kadikoy.org.tr/turksyip/verify/>

LAST SCAN DATE

2016-01-01 19:45:21

FILE CHECKSUM

SHA256 - f8b7fb00fac9af997e5252ee612f6cceacd3070e2ead4e5be8d4c5f7fcff5904

PAGE TITLE

Yahoo! Mail

HTML/CRYPTED.GEN

THREAT URL

<http://mhp-kadikoy.org.tr/turksyip/verify/>

LAST SCAN DATE

2016-01-01 19:45:21

FILE CHECKSUM

SHA256 - f8b7fb00fac9af997e5252ee612f6cceacd3070e2ead4e5be8d4c5f7fcff5904

PAGE TITLE

Yahoo! Mail

一个例子：0day变种病毒的发现



中国互联网安全大会



360互联网安全中心

1. 一个Office宏文件
2. 宏文件下载了一个Locky病毒的变种
3. 这个变种病毒试图链接服务器：79.170.44.88
4. 这个IP因为有恶意行为记录，已经被监视了.....
5. 根据恶意IP阻断这个链接，而不是根据病毒特征

Detail : <https://www.ixiacom.com/company/blog/ixia's-ati-research-center-protects-customers-another-zero-day-ransomware>

IP:79.170.44.88 **MALWARE**

RAP SHEET | LOCAL IP ADDRESSES | CONNECTION STATS

THREATS DETECTED: 2 MALWARE

HTML/TROJANCLICKER.IFRAME.NAG TROJAN

THREAT URL	http://mts.visionsgroup.co.uk/
LAST SCAN DATE	2016-07-23 12:45:06
FILE CHECKSUM	SHA256 - d4257e2c7acba4c427e9f17912fc04b213d00adb3488e37dc0514f109006ad46



JS/TROJANDOWNLOADER.AGENT.NXJ TROJAN

THREAT URL	http://www.folkestonewebhosting.com/_wp_scripts/jsRollover.js
LAST SCAN DATE	2016-07-23 12:44:43
FILE CHECKSUM	SHA256 - ae4d3328953c10356c16f49e8f8bc3f0131f05de675253d2e5e94c4eec0f6b2d

Reverse DNS: WEB88.EXTENDCP.CO.UK Last Blocked On: 2016-07-25 17:56:24



中国互联网安全大会



360互联网安全中心

LAB环境里再现真实世界流量

过去

- 网络数据抓包存储 + 高速网卡发送
- 昂贵，无状态，不可测量，不可控



在LAB里构造流量场景进行测试，开发，研究

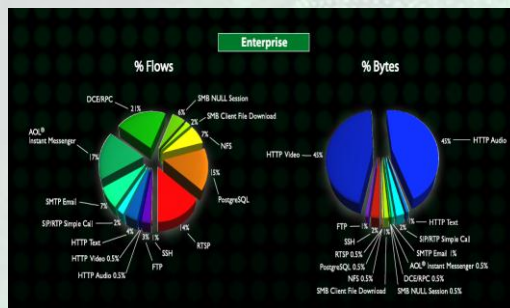


中国互联网安全大会



360互联网安全中心

- 三个要素：流量内容 + 流量形态 + 高性能
- 应用协议，典型应用程序，典型和自定义流量场景；实时更新.....



330+ 典型应用协议， 3500+ 典型的应用过程， ATI Aug 2016

- Markov动态可读文本

恶意流量仿真



中国互联网安全大会



360互联网安全中心

Environment

Lab Topology

Source Port Gateway Destination Port Gateway

Source Port IP Destination Port IP

Source Port		Destination Port	
IP Address:	Mask:	IP Address:	Mask:
81.128.0.1	24	81.128.0.2	24
Gateway:		Gateway:	
81.128.0.2		81.128.0.1	

This network simulates a group of client endpoints and a group of servers. In order to communicate to each other the hosts can go through a network inline device like a router or a transparent device that serves as the device under test.

Network details:

Two physical test interfaces are used to host the simulated clients and the servers respectively, which will be logically sitting behind virtual

Background Traffic

Attack Traffic

Map

Timeline

BreakingPoint Enterprise

ClientSim HTTP Slow...

ClientSim HTTP Slow Headers#2

0 20 40 60 80 100 120 140

Test Status Export Import Reset Defaults Save Save As Run

7000+ 典型BOTNET/DNAs过程QIP归属位置仿真 (Aug2016)

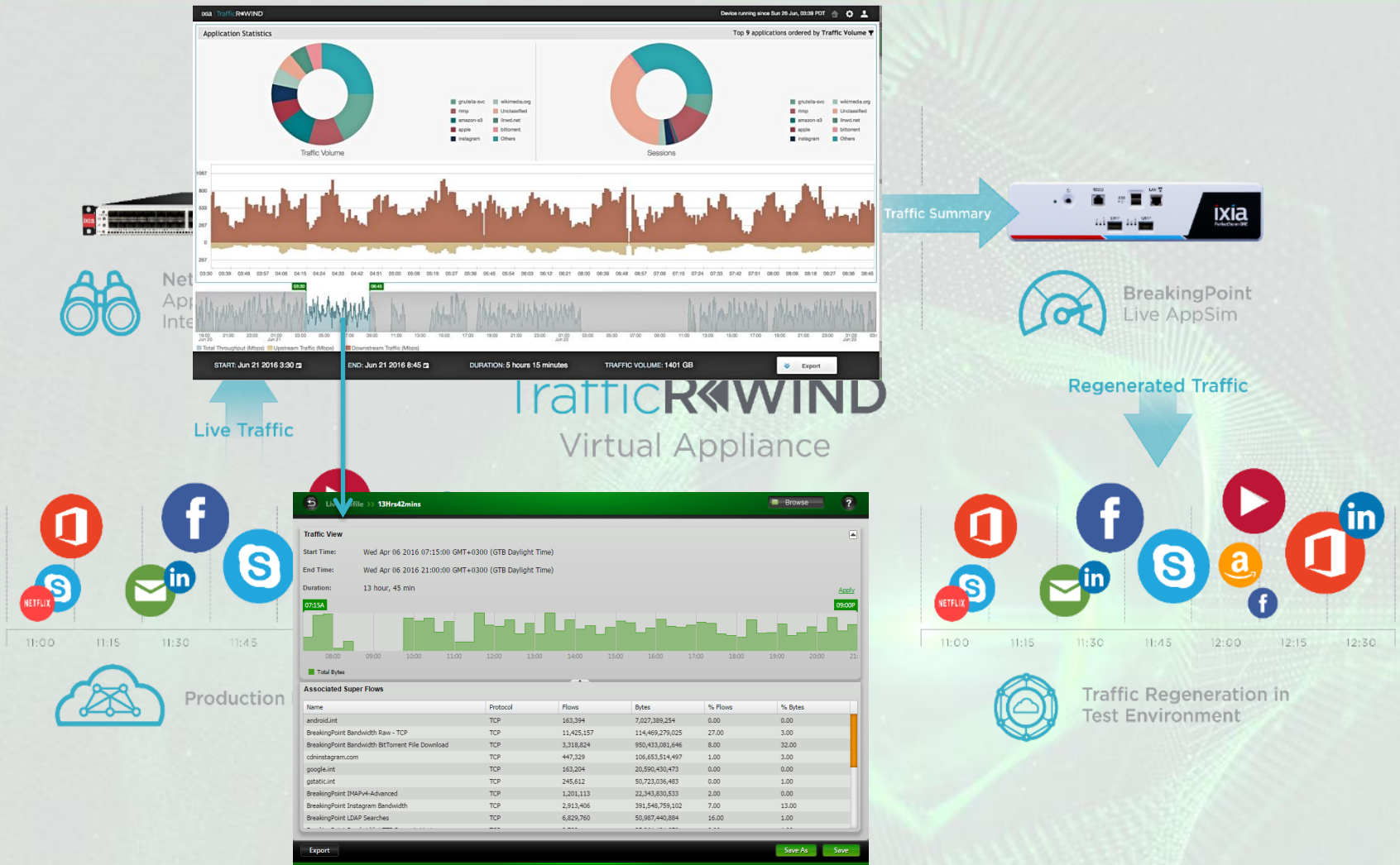
对生产网络的流量实时记录并重现



中国互联网安全大会



360互联网安全中心



7天时长的大容量记录，5千万倍压缩比重现流量，



中国互联网安全大会



360互联网安全中心

ixia

2nd August 2016

ATI NEWSLETTER



RELEASE HIGHLIGHTS

- Ixia launches TrafficREWIND™— [Blog: The Bridge Between Production Networks and Testing Labs](#)
- Ixia's Application and Threat Intelligence (ATI) Research Center exposes (another) [zero-day ransomware](#)
- Introduction of apps like Google Cache and Google Keep provides holistic coverage of Google apps in Ixia ATI
- ATI's war against malwares continues with the support of the vicious android malware [Godless](#) and ransomwares like [Locky](#) (newer version), [Satana](#), and [TorrentLocker](#)
- ATI adds support of [BaiduTieba](#), the largest Chinese communication platform provided by Baidu
- ATI includes newer Sandvine Application profiles emulating North America and Latin Americas Fixed and Mobile traffic
- ATI Evergreen program updates AOL Mail & Chat, Gmail, Rediffmail, Yahoo Mail & Chat, Twitter, Facebook to latest version

实时更新推送给用户

谢 谢



中国互联网安全大会



360互联网安全中心