RSA移动安全面面观

安天实验室.AntiyLabs
Tom:Pan
tompanpan@gmail.com

提纲

- 从RSA展会的角度
- 从趋势数据的角度
- 从企业发展的角度
- 从安全需求的角度
- 思考和总结

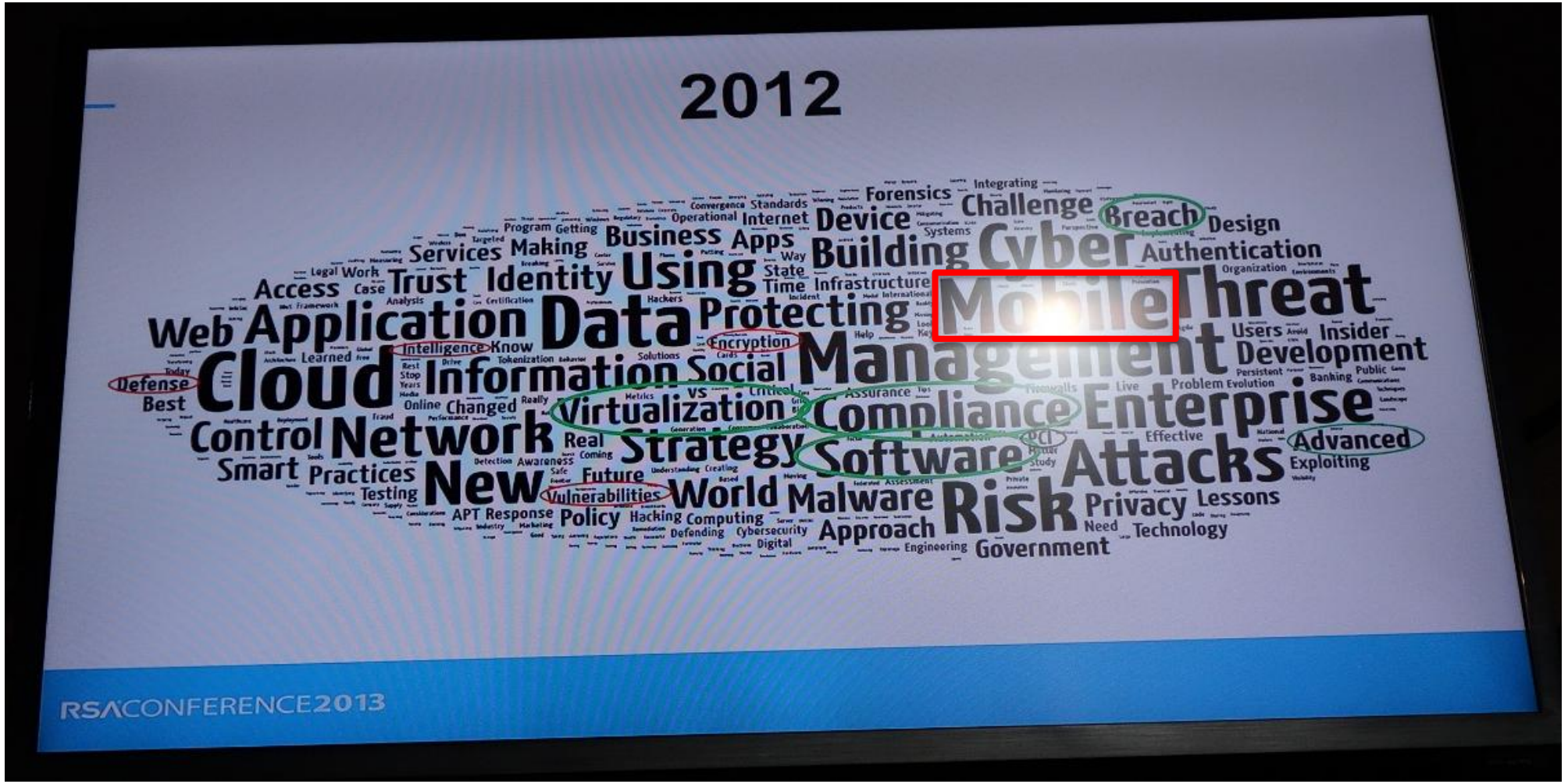
RSA展会的角度

从过去几年RSA展会的角度看移动安全阵营

RSA 2011


2011
Using
Malware
Infrastructure
Framework
Vulnerability
Software
Cyber
Data
Building
Authentication
Key
Technology
Trusted
Privacy
Analysis
Monitoring
Protecting
Practices
Enterprise
Web
Social
Lessons
Service
Making
Risk
Management
Cloud
Devices
Development
Strategy
Real
Effective
Wireless
Encryption
Application
Identity
Network
World
Challenges
Business
Lifecycle
Case
Integrated
Public
Access
Mobile
Based
Program
Information
Compliance
Threat
Future
Control
War
Attacks
New
Intelligence
Implementing
Best
Impact
Environment
Approach
Solutions
User
RSACONFERENCE2013

RSA 2012


2012
Forensics
Integrating
Challenge
Breach
Design
Convergence
Standards
Operational
Internet
Device
Systems
Program
Getting
Business
Apps
Services
Making
Building
Cyber
Authentication
Way
Legal
Work
Trust
Identity
Using
State
Infrastructure
Access
Case
Time
Mobile
Threat
Web
Application
Data
Protecting
Users
Insider
Intelligence
Know
Encryption
Development
Learned
Tokenization
Social
Management
Defense
Information
Problem
Evolution
Best
Online
Changed
Virtualization
Compliance
Enterprise
Control
Network
Real
Strategy
Effective
Advanced
Smart
Practices
Awareness
Future
Software
Attacks
Exploiting
New
Testing
Vulnerabilities
World
Malware
Risk
Privacy
Lessons
APT
Response
Policy
Hacking
Computing
Need
Technology
Defending
Cybersecurity
Approach
Digital
Engineering
Government
RSACONFERENCE2013

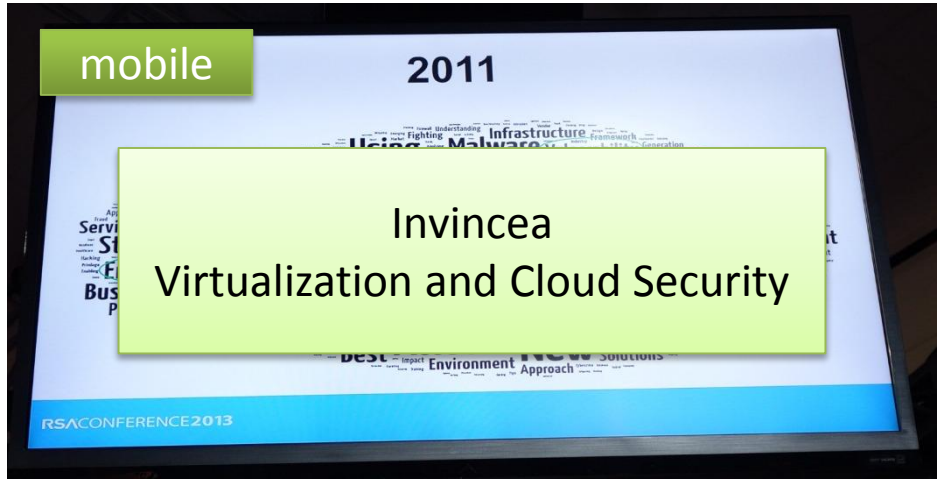
RSA 2013

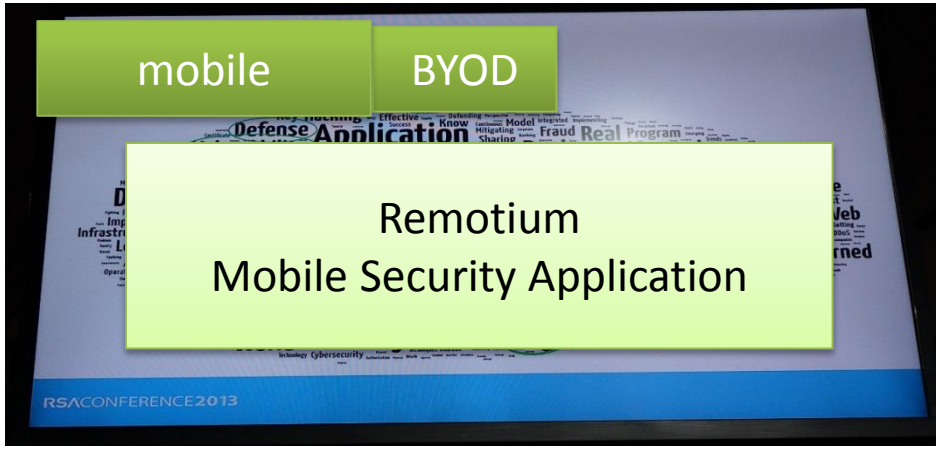

2013
Key Hacking
Defense
Application
Vulnerability
Intelligence
Network
Business
Approach
Service
Fraud
Real
Program
Detection
Solutions
Privacy
Encryption
Analysis
Devices
Attacks
Strategy
Virtual
Enterprise
Malware
Future
Control
Web
Management
Cloud
Threats
Using
Legal
Apps
Protection
Mobile
Information
Building
Learned
Insider
Code
Risk
Cyber
Data
New
BYOD
Advanced
Lessons
Development
Authentication
Big
Social
Trust
Compliance
World
Identity
Practices
Testing
Infrastructure
Improving
Prevention
Challenges
Automated
Software
Public
Response
Policy
Cybersecurity
RSACONFERENCE2013

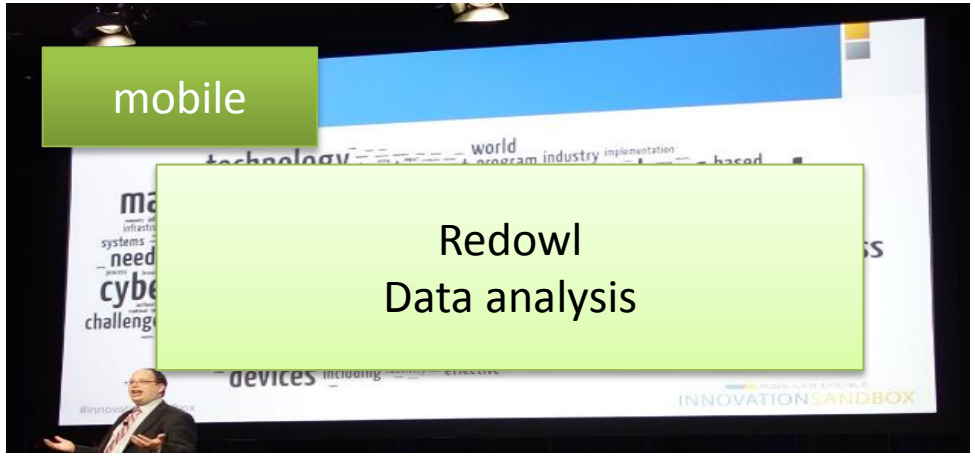
RSA 2014


2014
technology
development
world
program
industry
implementation
approach
based
cloud
management
share
malware
help
detection
threats
new
users
tools
data
control
government
work
software
real
practices
systems
need
critical
organizations
risk
business
access
cyber
privacy
solutions
attacks
mobile
information
challenges
time
protect
applications
enterprise
network
vulnerabilities
services
operations
devices
including
identity
effective
requirements
INNOVATIONSANDBOX

RSA 2011 ~ 2014



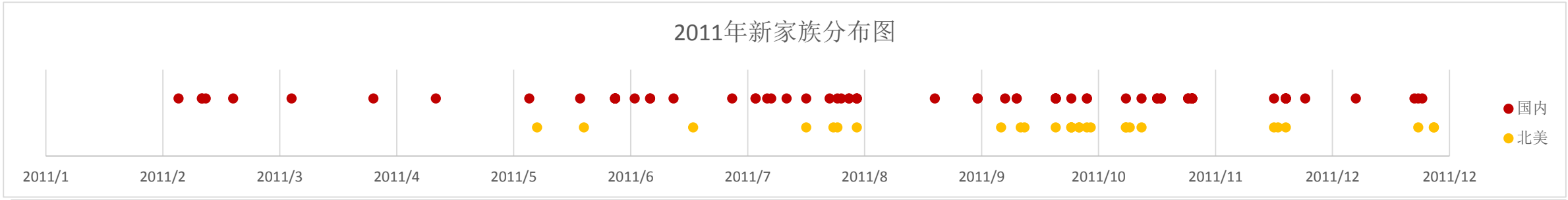


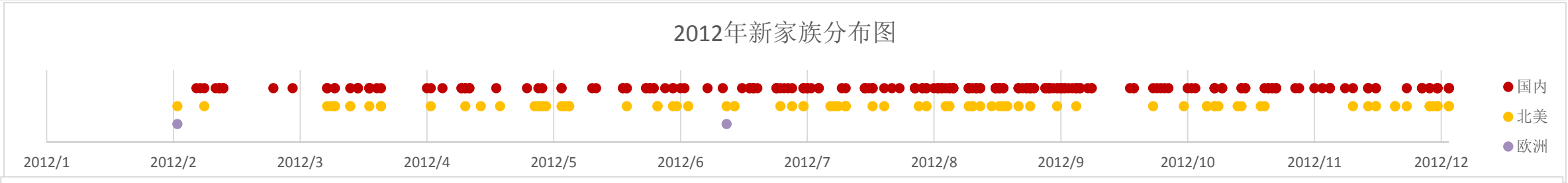


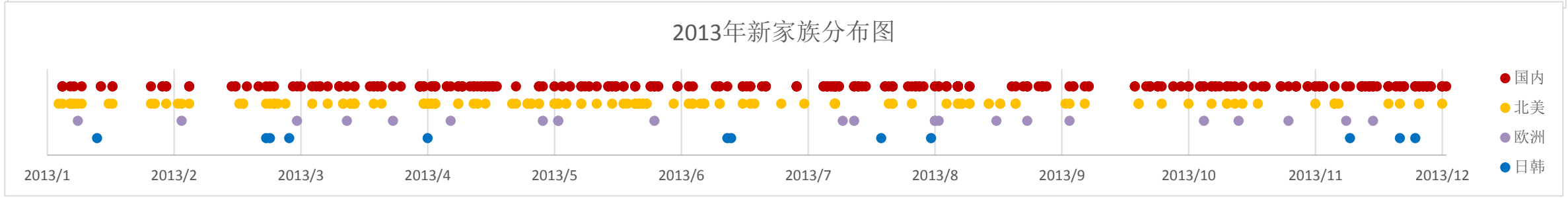
趋势数据的角度

我们再从数据的角度，看看过去几年的移动安全形势

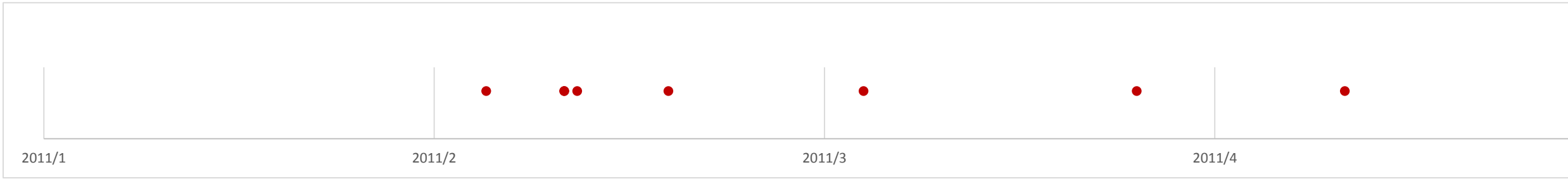
2010~2013年恶意代码变迁

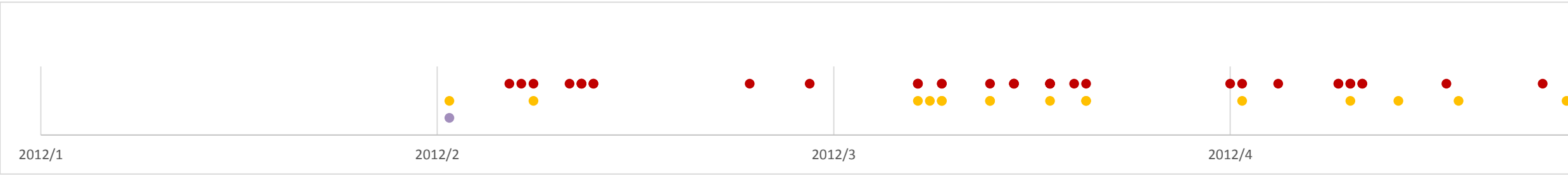


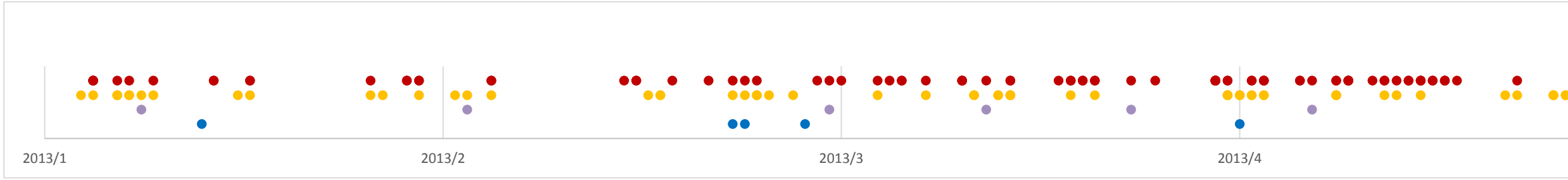


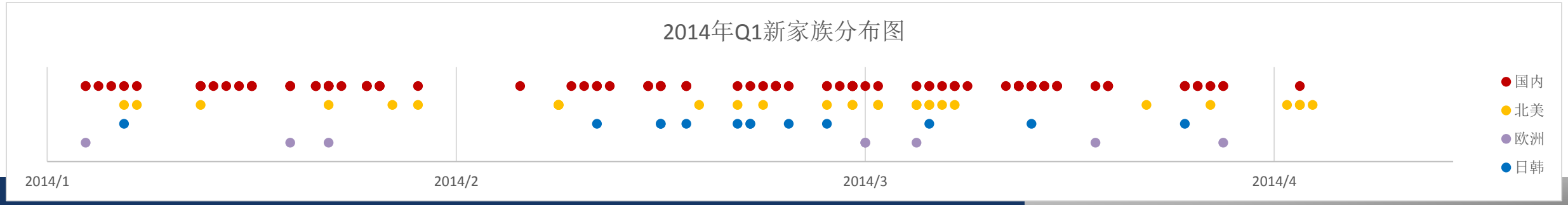


2010~2013年恶意代码变迁

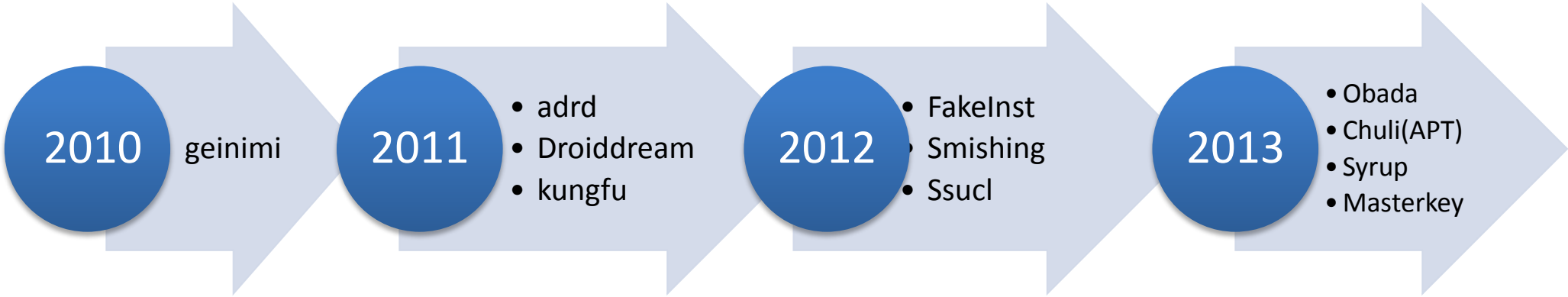


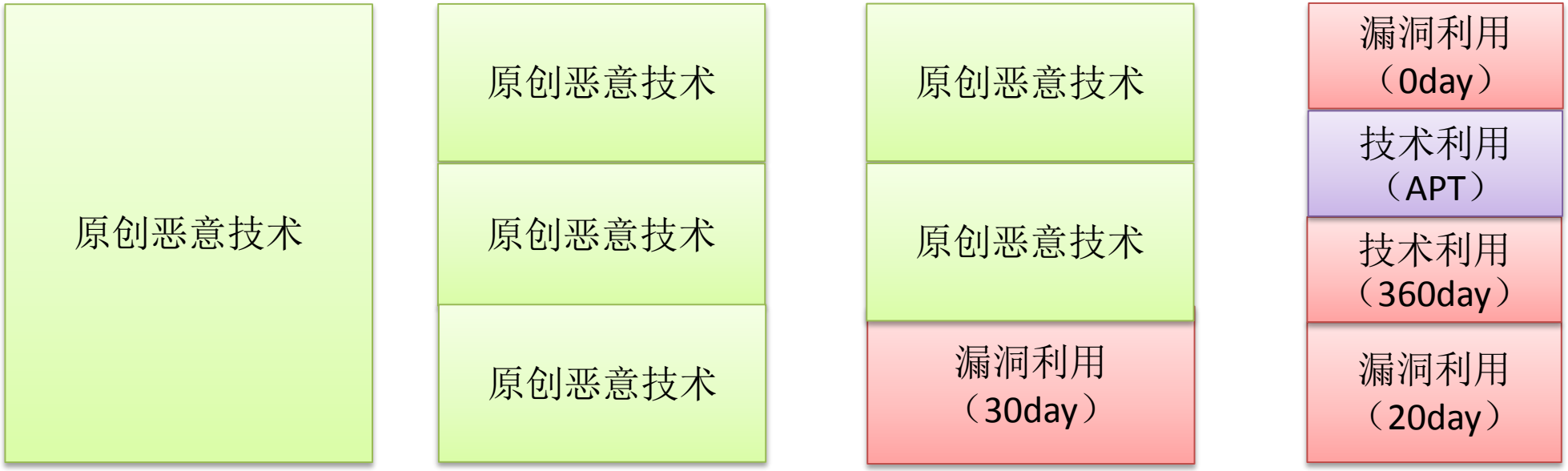






2010~2013年恶意代码技术脉络





企业发展的角度

从国内外企业发展的角度看移动安全的发展

RSA 2012 ~ 2014

RSA 2012

- 个人
  - AhnLab
- 企业
  - AirWatch
  - BluePoint
  - ForeScout
  - Pindrop
- 开发者
  - Arxan
- 创新沙盒获奖
  - Appthority
  - 较多移动相关

RSA 2013

- 个人
  - 较多，超过5家
- 企业
  - AirWatch
  - Bluepoint
  - Damballa
  - FireEye
  - MobileIron
  - Mocana
  - Zenprise
  - Pindrop
- 开发者
  - Arxan
- 创新沙盒获奖
  - Remotium安全应用
  - 较多移动相关

RSA 2014

- 个人
  - 太多，超过10家
- 企业
  - Appthority
  - Mocana
  - MobileIron
  - Bluebox
  - Veracode
  - FireEye
- 开发者
  - Arxan
- 创新沙盒获奖
  - RedOwl

RSA 公司盘点

Application

- Remotium

Antivirus&Protection

- Lookout， Bluepoint

BYOD/MDM

- AirWatch， MobileIron， Mocana， Zenprise

Service

- Appthority， PinDrop， Veracode

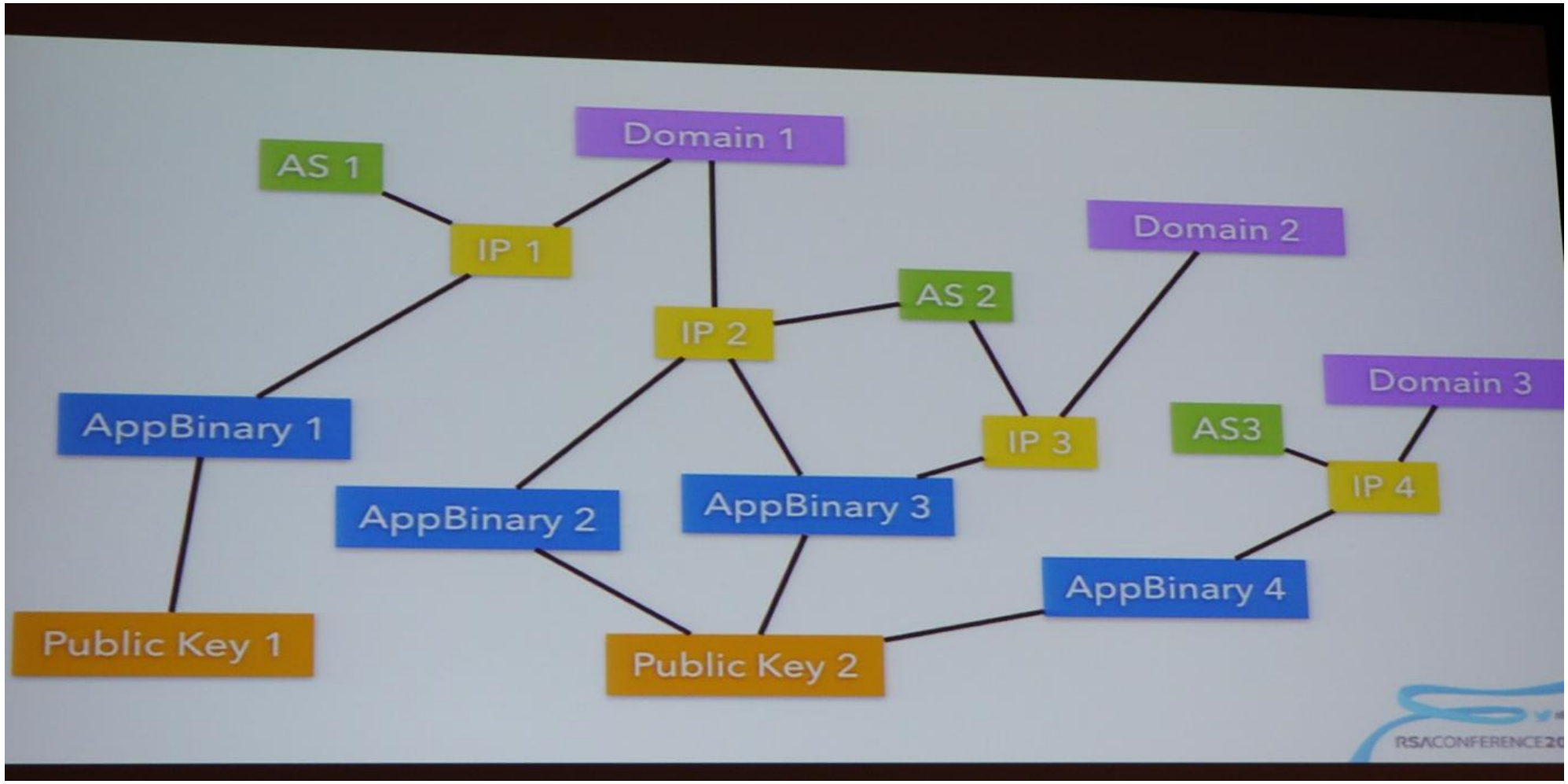
Solution

- PANW,FireEye,……

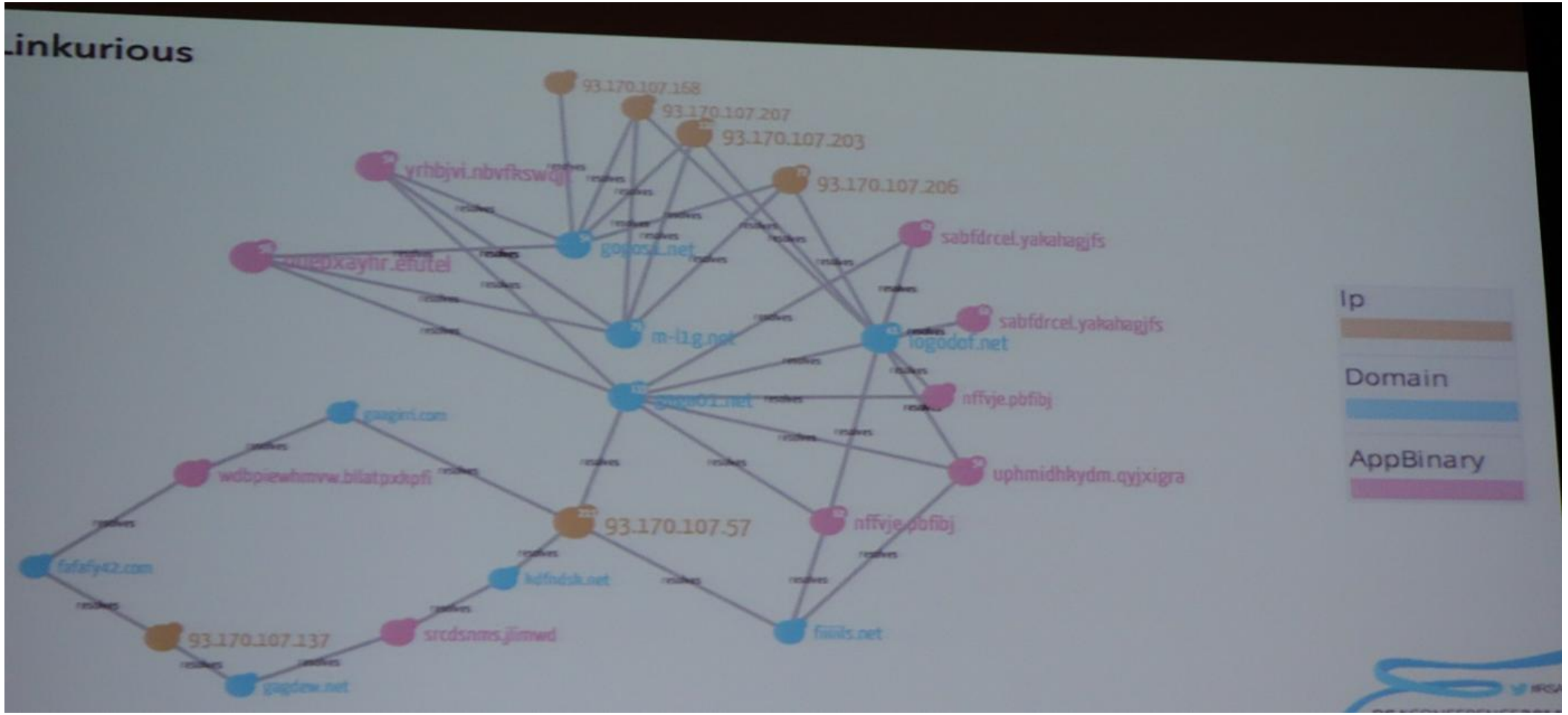
海外移动安全团队

- Lookout
  - 2009年开始，持续占据北美和海外个人安全软件头名
  - 超过100人工程师团队
- FireEye
  - 2012开始围绕Dawn Song进行移动安全团队组建，目前吸引了包含多名华人学者的超过40人的工程师团队
  - 2012年发布了基于污点追踪的Android动态分析沙箱产品原型
- Palo Alto Network
  - 2012年在WildFire中加入对移动的支持，并在APP-ID上加入对部分移动的支持
  - 2012开始和MobileIron，Citrix合作
- Bluebox
  - 1篇博客的力量，宣布发现MasterKey漏洞，声名大噪
  - 发布企业移动安全解决方案
- 蒋旭宪老师研究团队
  - 2011，2012多次首发多个Android恶意代码家族和漏洞
- Start-up&Other
  - Appthority
  - Veracode
  - Trustlook，VisualThreat
  - Zimperium，lacoon

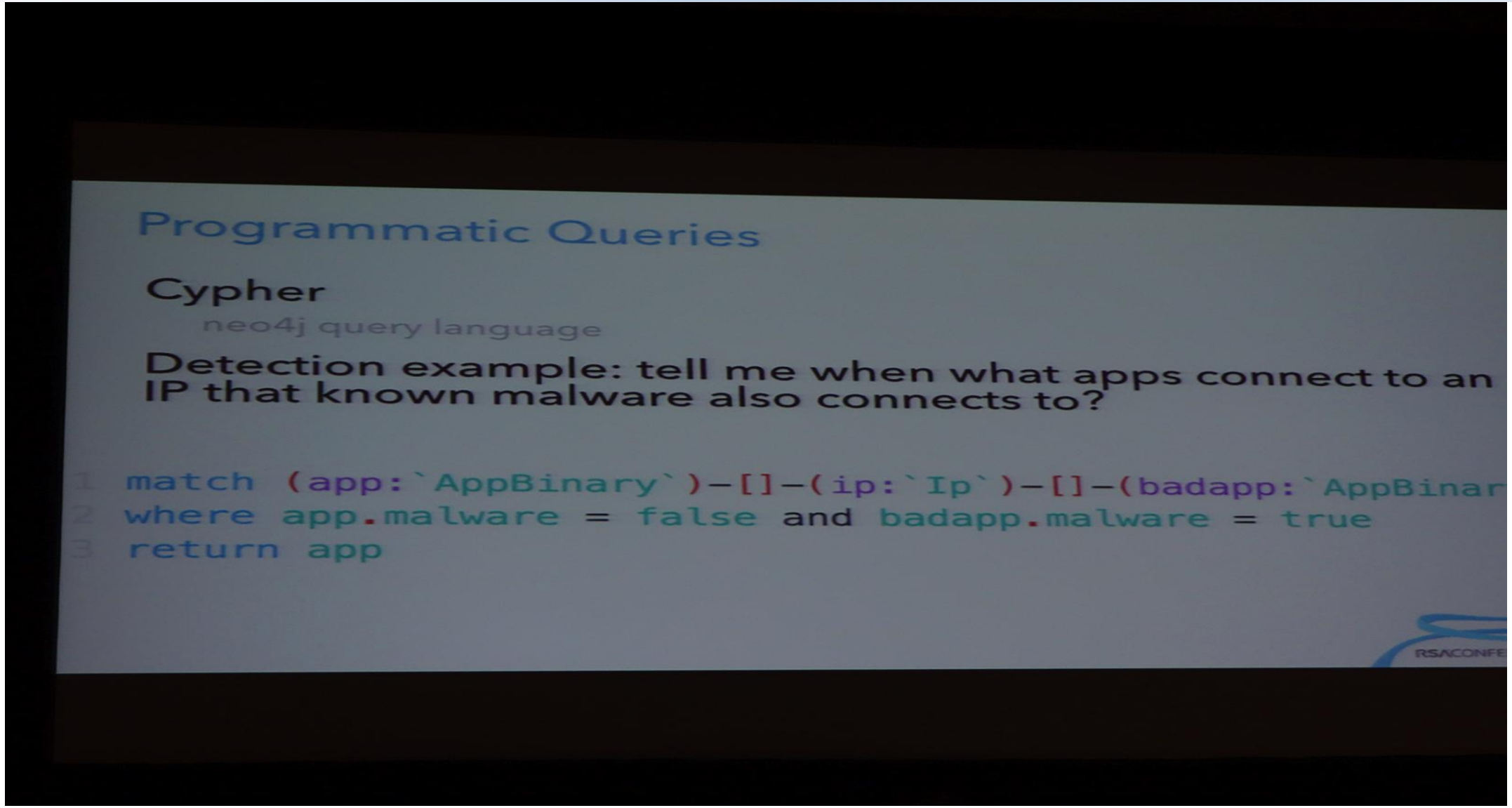
Lookout的可视化分析



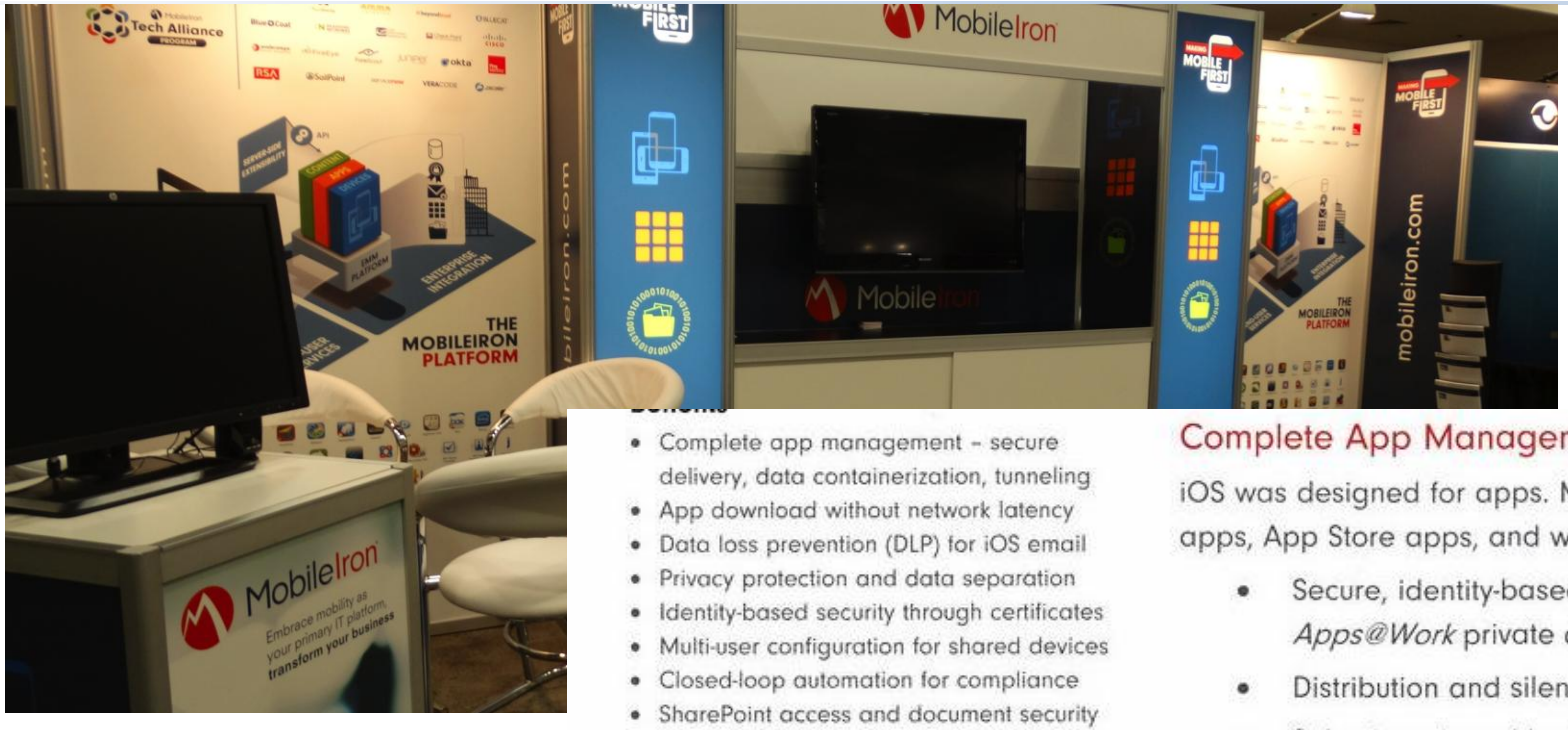
Lookout的可视化分析



Lookout的可视化分析



MobileIron的技术特点



统一平台

SDK支持

- Complete app management – secure delivery, data containerization, tunneling
- App download without network latency
- Data loss prevention (DLP) for iOS email
- Privacy protection and data separation
- Identity-based security through certificates
- Multi-user configuration for shared devices
- Closed-loop automation for compliance
- SharePoint access and document security
- Cost control thru monitoring of int'l roaming
- Enterprise integration thru extensible APIs
- Single-system scale of 100,000 devices
- Multi-tier management for delegation
- Best-in-class for cloud and on-premise

Recent Recognition

Gartner: MobileIron positioned in the Leaders Quadrant of the Magic Quadrant for Mobile Device Management Software (May 2012)

Info-Tech: MobileIron listed as a Champion in the Mobile Device Management Suites

Complete App Management

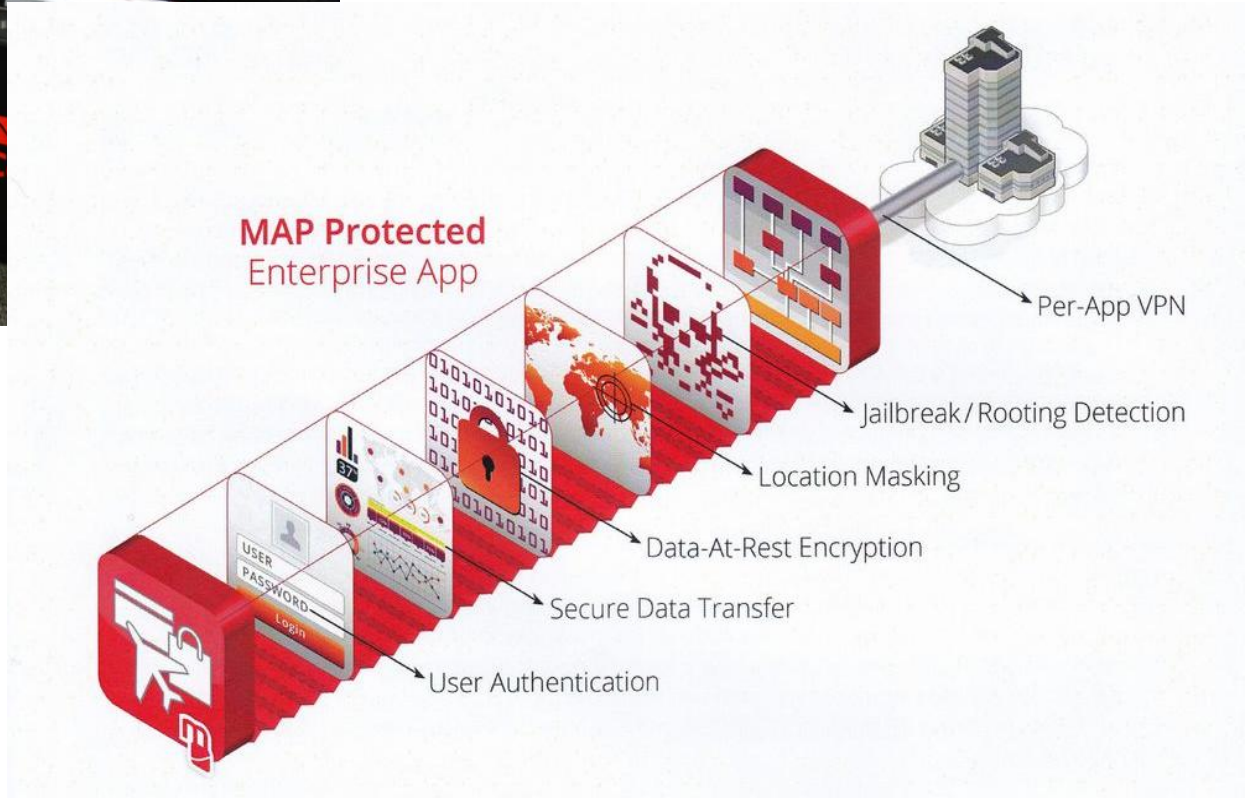
iOS was designed for apps. MobileIron provides app management for in-house apps, App Store apps, and web apps:

- Secure, identity-based delivery of in-house and App Store apps through the *Apps@Work* private app storefront
- Distribution and silent install of HTML apps as Web Clips
- Selective wipe of business apps and apps data on the device
- Blacklist/whitelist of apps to protect against inappropriate access or use
- Integration with the App Store Volume Purchase Program (VPP)
- App download through the *App Delivery Network* (AppDN) to minimize network load and provide fast downloads for the end user
- Containerization and dynamic policy to protect data-at-rest and enable compelling app-based user experiences through *AppConnect**
- Secure tunneling to protect data-in-motion through *AppTunnel**

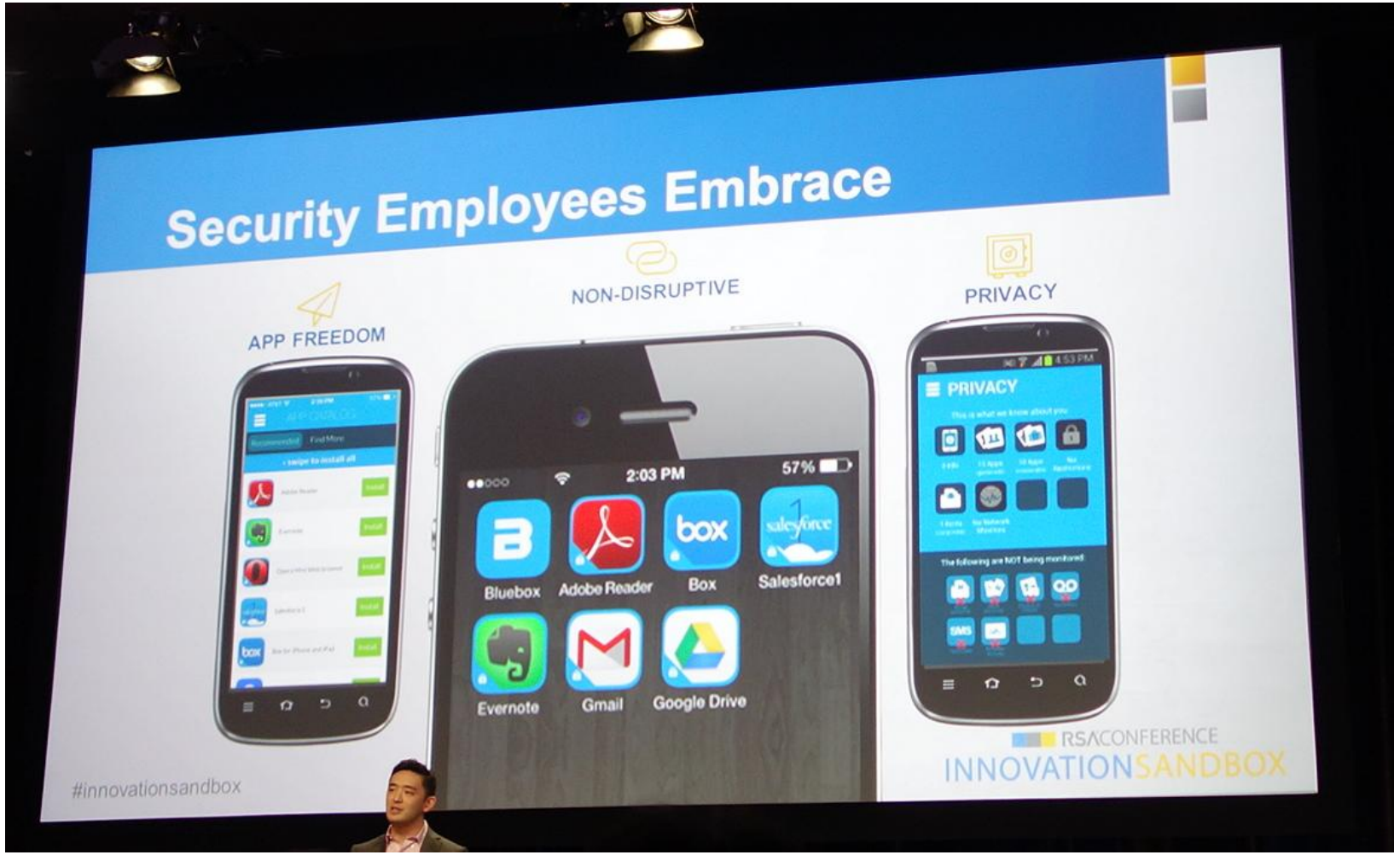
Mocana的技术特点

控制通路

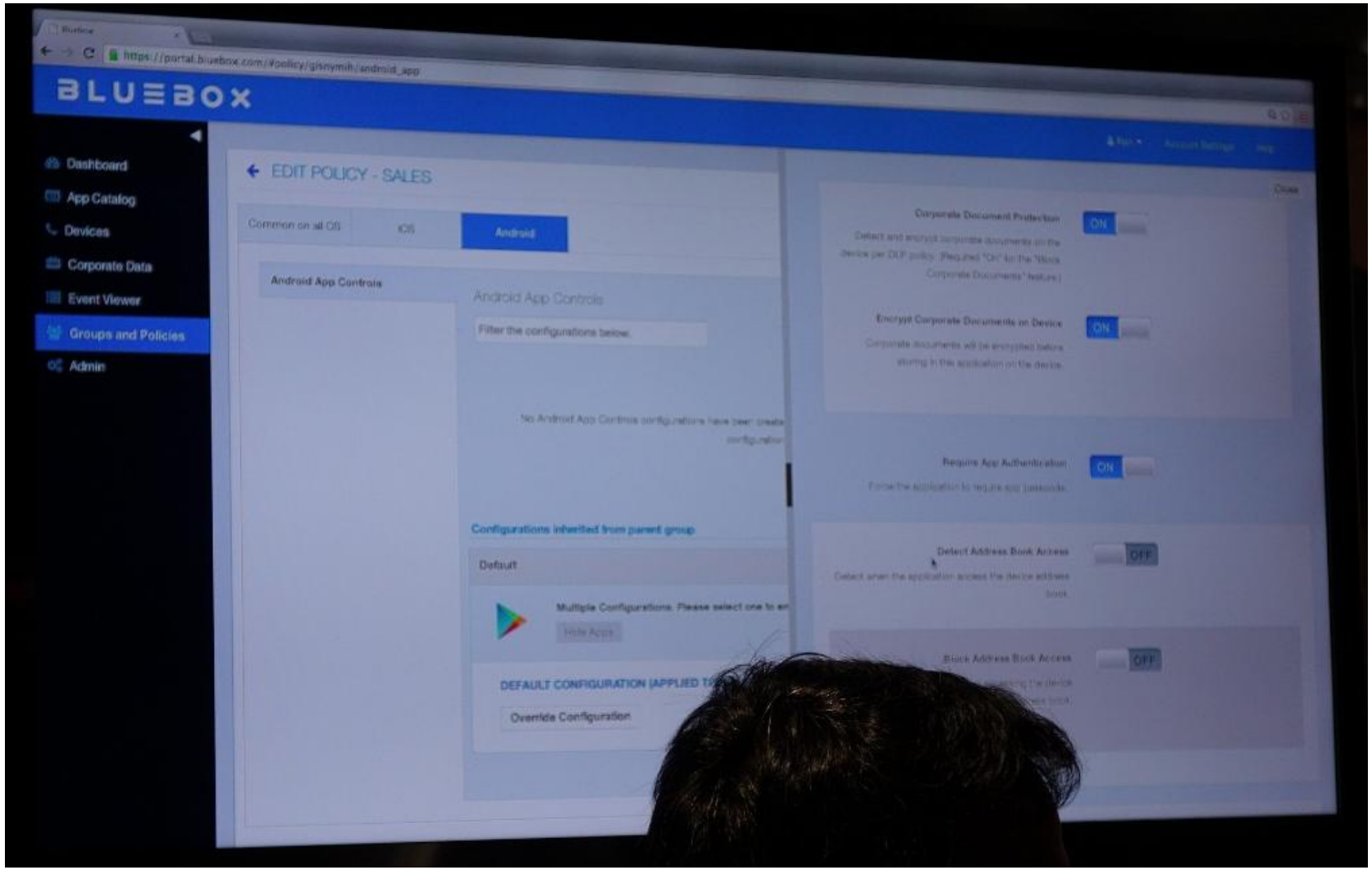
透明便利



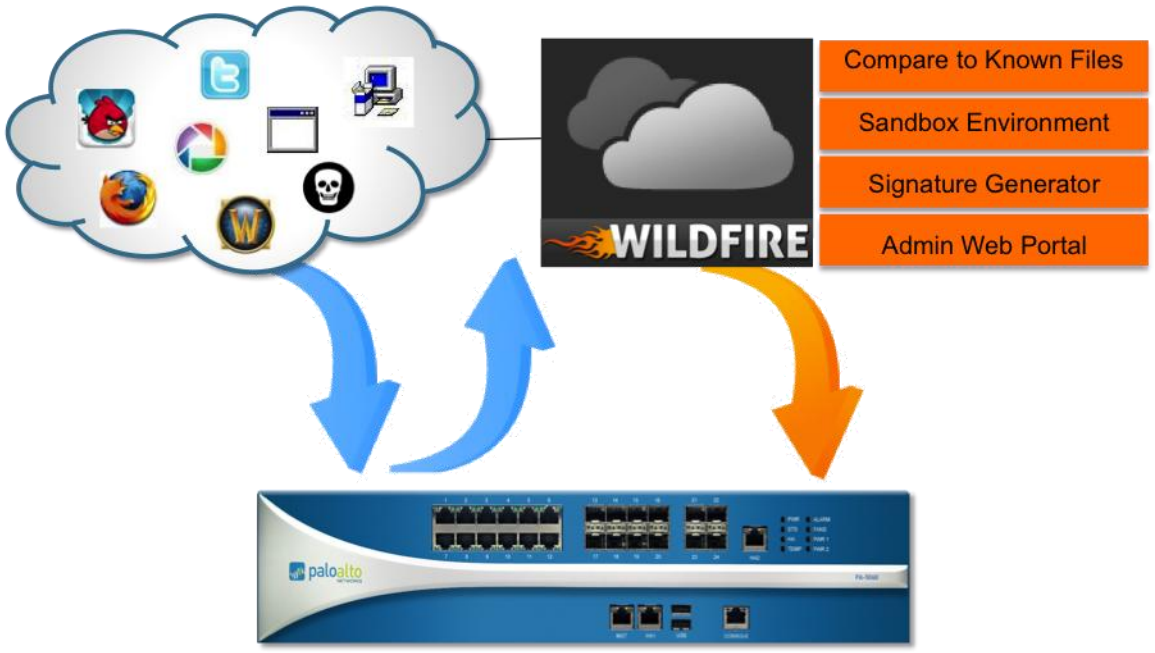
Bluebox的安全Context Container技术



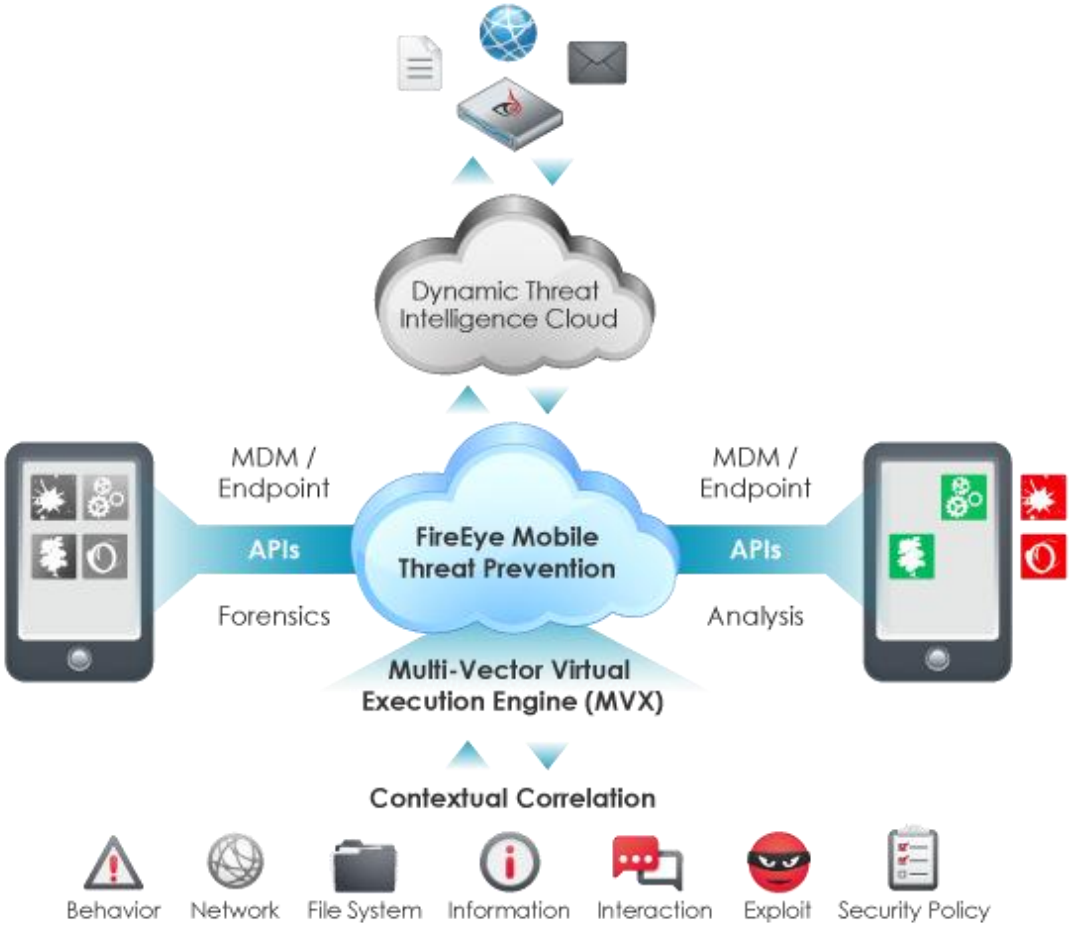
Bluebox的安全Context Container技术



FireEye&PANW



WildFire



MobileThreatPrevention

Start-up/Other

Appthority Trust Your Apps

应用安全风险管理

trustlook

Mobile APT

VisualThreat

Analysis Service

VERACODE

Audit Service

ZIMPERIUM MOBILE DEFENSE

Mobile IPS

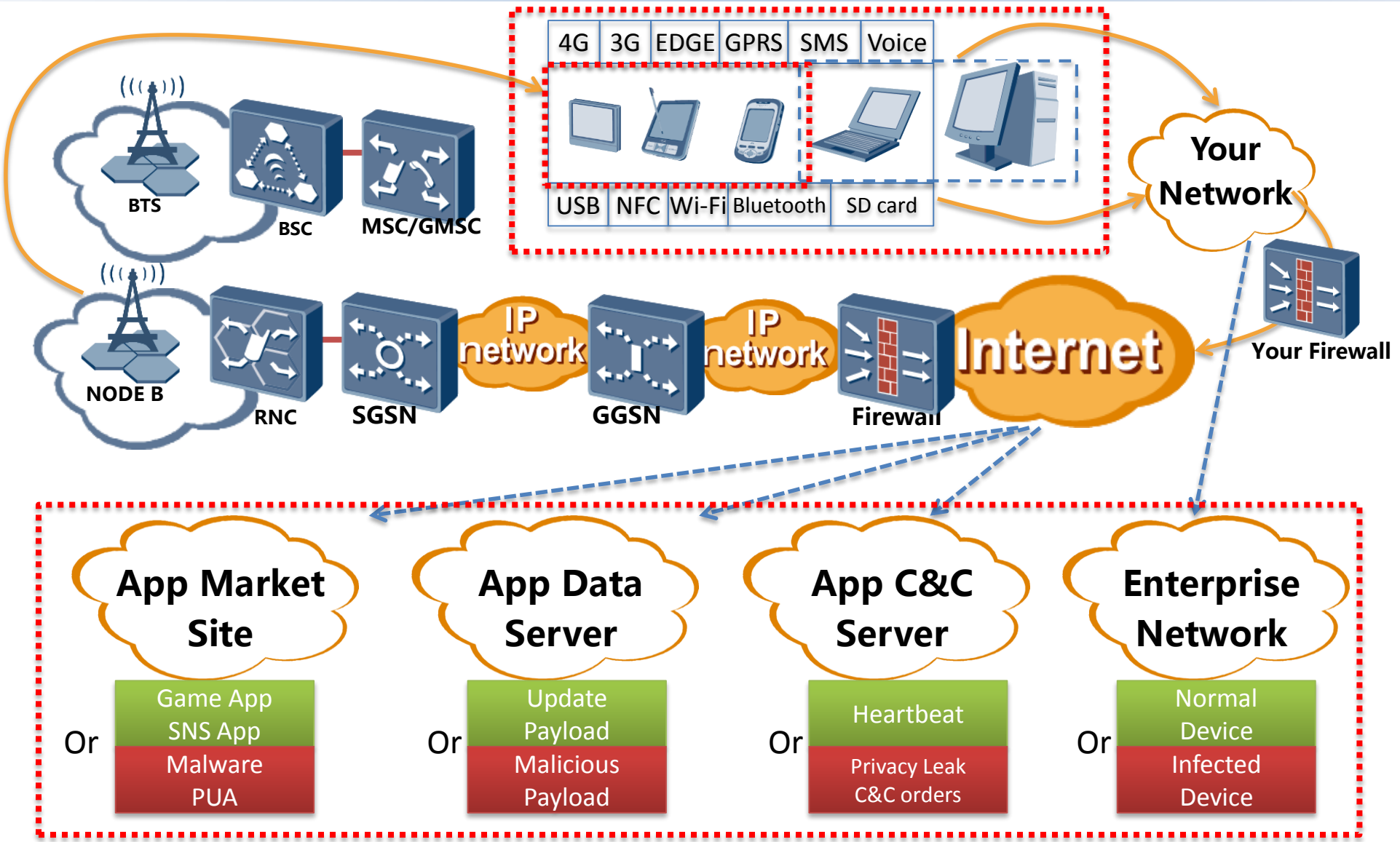
LACOON MOBILE SECURITY

Behavior-ed Based

安全需求和技术的角度

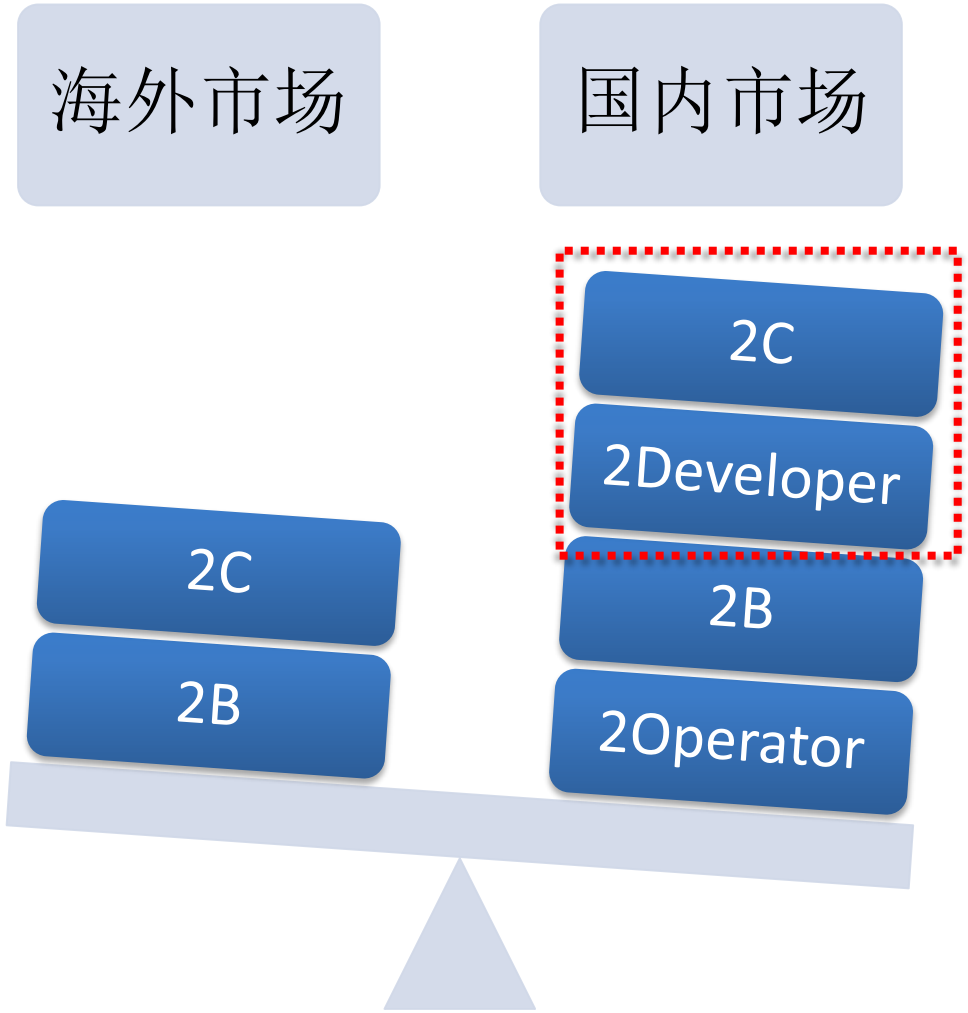
安全需求和技术在中国和海外差异巨大

移动安全的挑战


4G
3G
EDGE
GPRS
SMS
Voice
USB
NFC
Wi-Fi
Bluetooth
SD card
BTS
BSC
MSC/GMSC
NODE B
RNC
SGSN
IP network
GGSN
IP network
Firewall
Internet
Your Network
Your Firewall
App Market Site
Or
Game App
SNS App
Malware
PUA
App Data Server
Or
Update Payload
Malicious Payload
App C&C Server
Or
Heartbeat
Privacy Leak
C&C orders
Enterprise Network
Or
Normal Device
Infected Device

海外和国内的需求差异

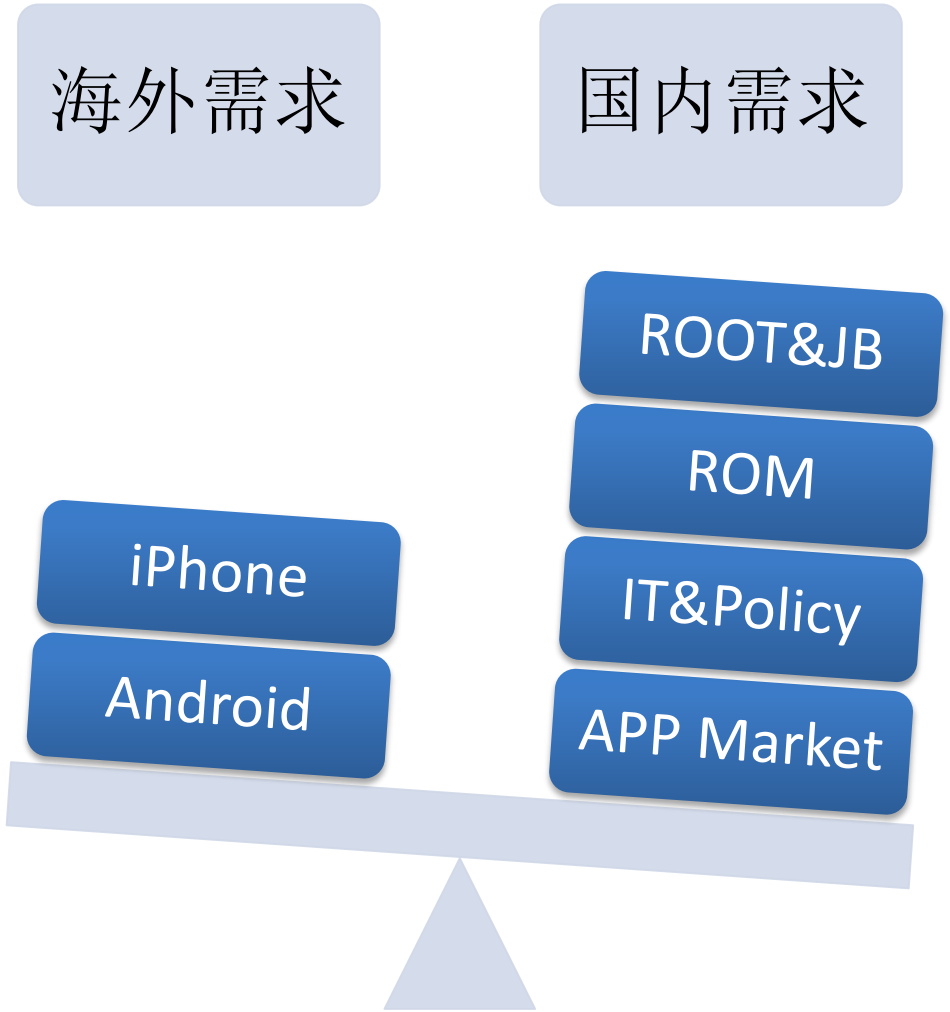
- 企业级安全为最大市场和需求
- 个人安全主要被传统PC安全厂商重新划分
- 技术创新一般，但商业思路成熟



- 个人安全是最大的市场和竞争，安全全面走向范安全化
- 企业级安全的市场需求短期还是在观望
- 安全需求和产品覆盖面和模式丰富
- 技术创新丰富，高效，但商业成熟度还需要时间

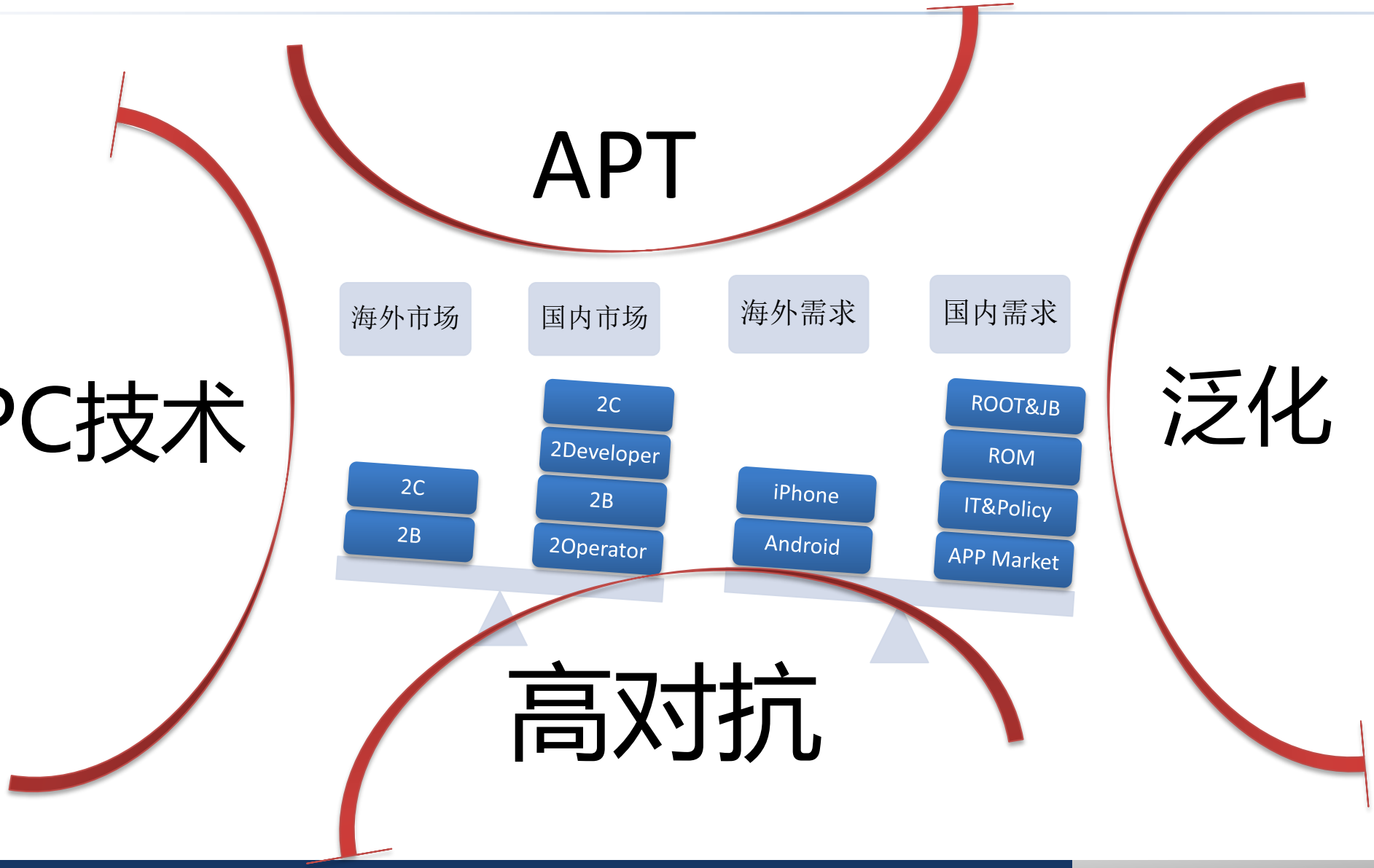
海外和国内的技术需求差异

- iPhone成为刚需求
- Google/Android在持续更新，并调整安全策略



- 越狱提权
- ROM和碎片化
- 行业策略和企业治理，版权保护
- 应用分发渠道发达

移动安全挑战


APT
PC技术
泛化
高对抗
海外市场
国内市场
海外需求
国内需求
2C
2B
2C
2Developer
2B
2Operator
iPhone
Android
ROOT&JB
ROM
IT&Policy
APP Market

重新思考
重新构建
新生

移动安全新生进行中

tompan@antiy.cn
Tom:Pan AntiyLabs Mobile Team