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

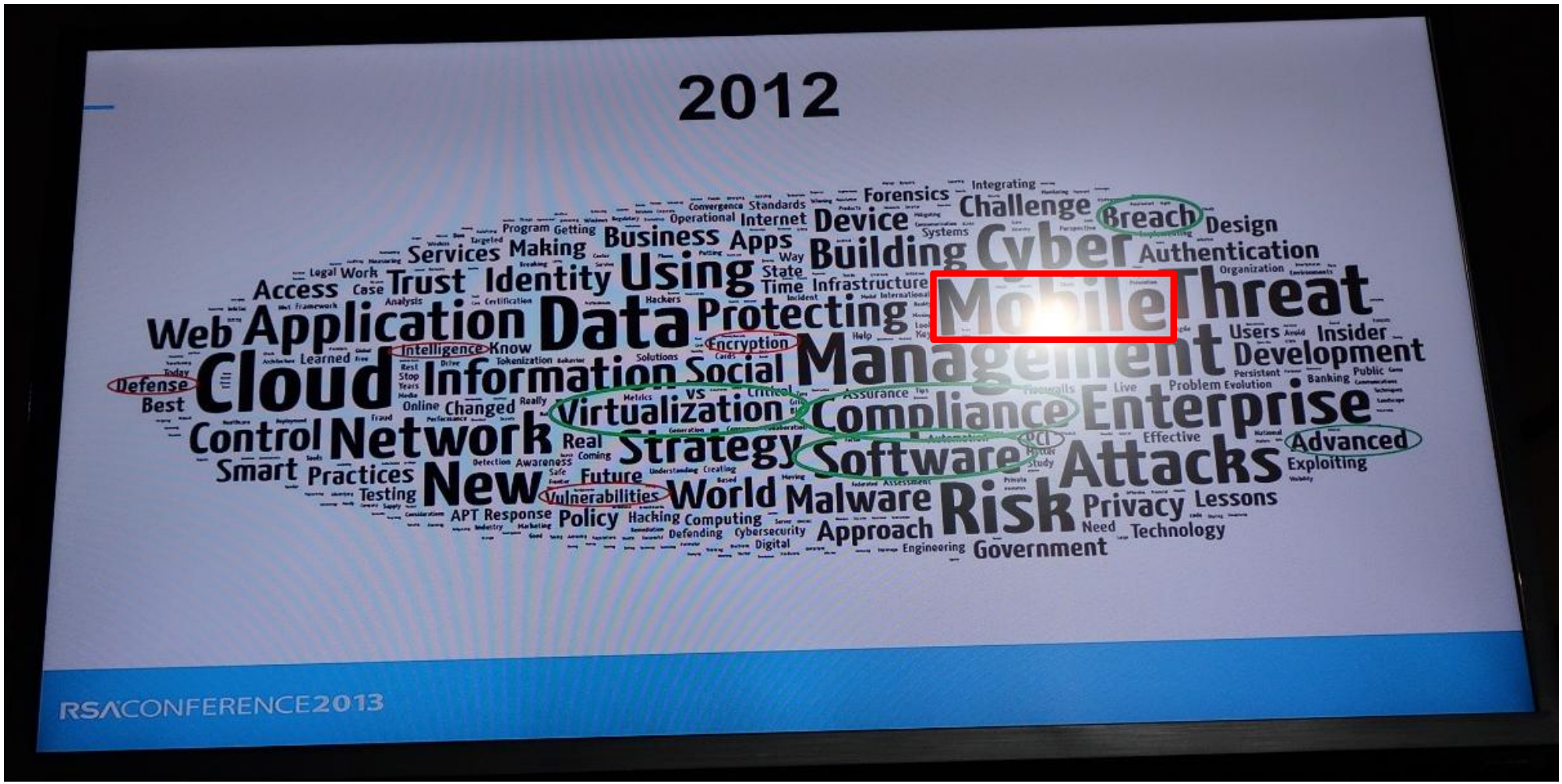
RSA展会的角度

从过去几年RSA展会的角度看移动安全阵营

SA 2011


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

SA 2012


2012
Cloud
Application
Data
Management
Cyber
Mobile
Threat
Network
Information
Enterprise
Compliance
Virtualization
Software
Attacks
Risk
Strategy
Building
Using
Protecting
Identity
Trust
Access
Web
Social
Big
Challenge
Breach
Device
Internet
Business
Apps
Services
Making
Authentication
Design
Development
Users
Insider
Encryption
Intelligence
Know
Defense
Best
Changed
Online
Control
Smart
Practices
Testing
New
Real
Future
Vulnerabilities
World
Malware
Advanced
Exploiting
Privacy
Lessons
Technology
Need
Approach
Government
Policy
Hacking
Computing
Defending
Cybersecurity
Digital
APT
Response
Awareness
Detection
Forensics
Integrating
Standards
Operational
Convergence
Program
Getting
Targeted
Making
Work
Legal
Case
Analysis
Certification
Hackers
Time
State
Way
Infrastructure
Incident
Organization
Systems
Tokenization
Solutions
Cards
Help
Live
Problem
Evolution
Persistent
Banking
Public
Effective
Assurance
Critical
Metrics
vs
Rest
Stop
Years
Media
Today
Drive
Fraud
Performance
Coming
Safe
Understanding
Creating
Based
Assessment
Private
Study
Engineering
RSACONFERENCE2013

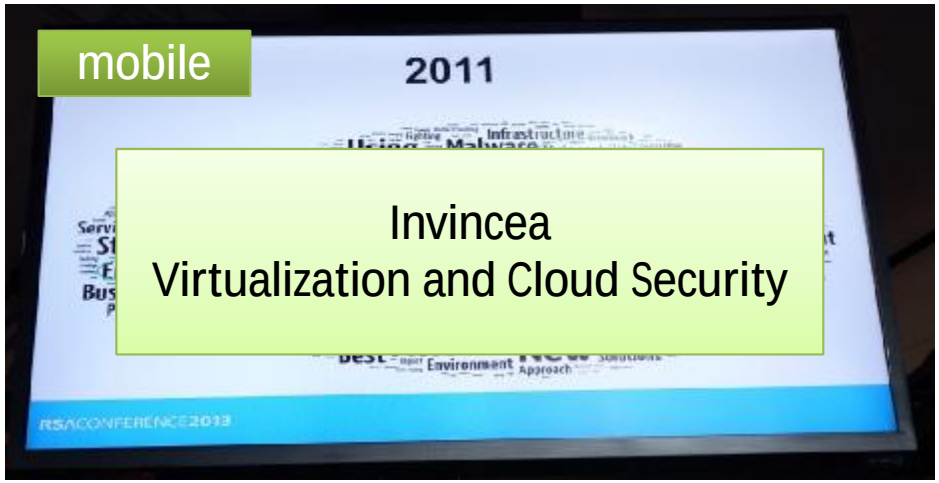
SA 2013


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

SA 2014


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

SA 2011 ~ 2014


mobile
2011
Invincea
Virtualization and Cloud Security


mobile
2012
Appthority
Mobile Security Service

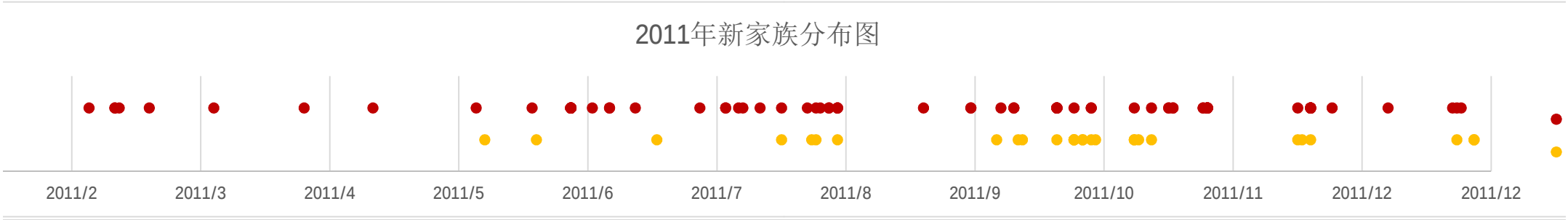

mobile
BYOD
Remotium
Mobile Security Application

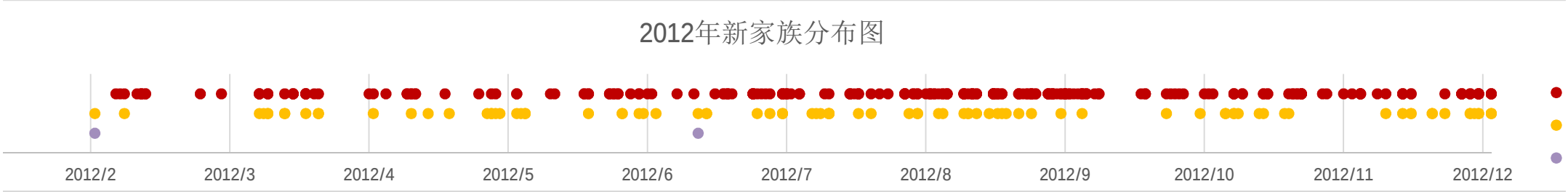

mobile
Redowl
Data analysis

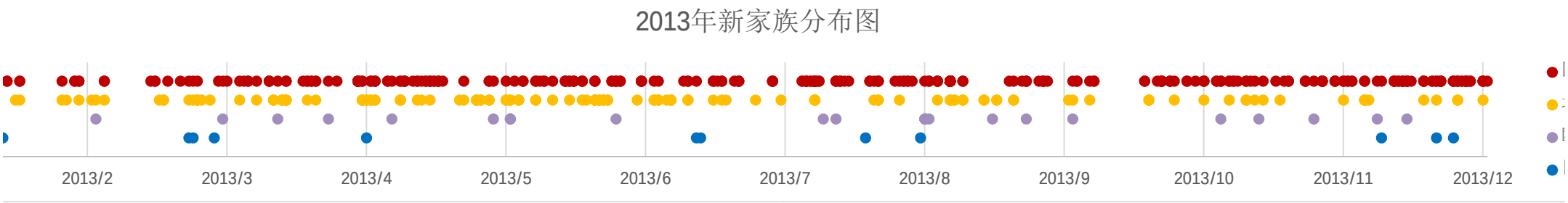
趋势数据的角度

我们再从数据的角度，看看过去几年的移动安全形势

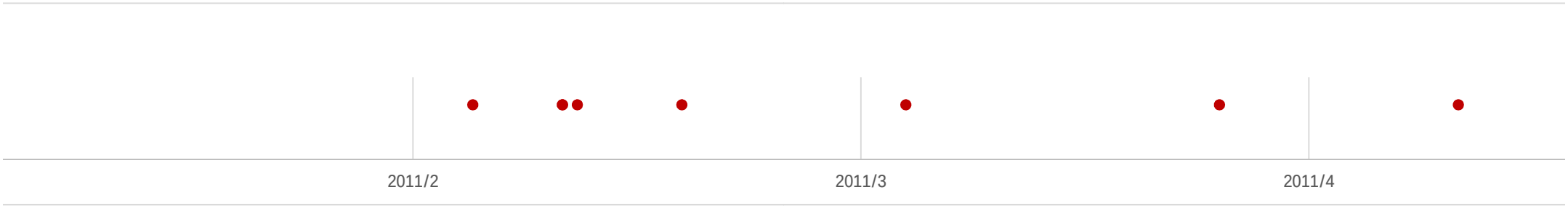
010~2013年恶意代码变迁

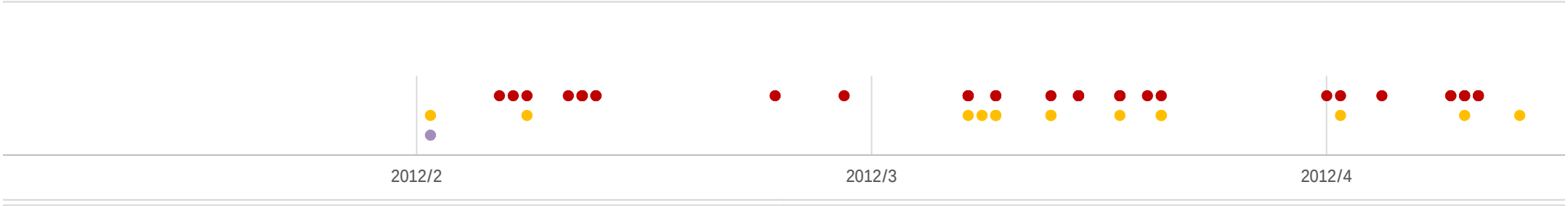


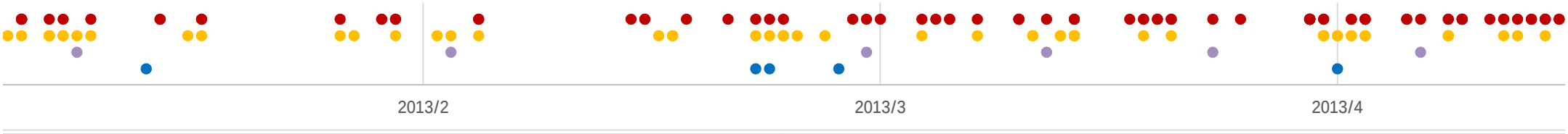




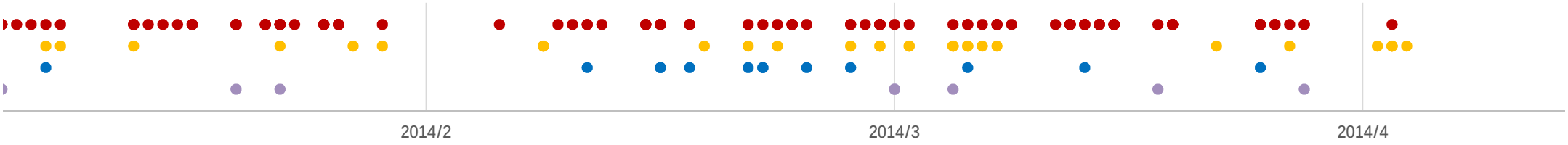
010~2013年恶意代码变迁



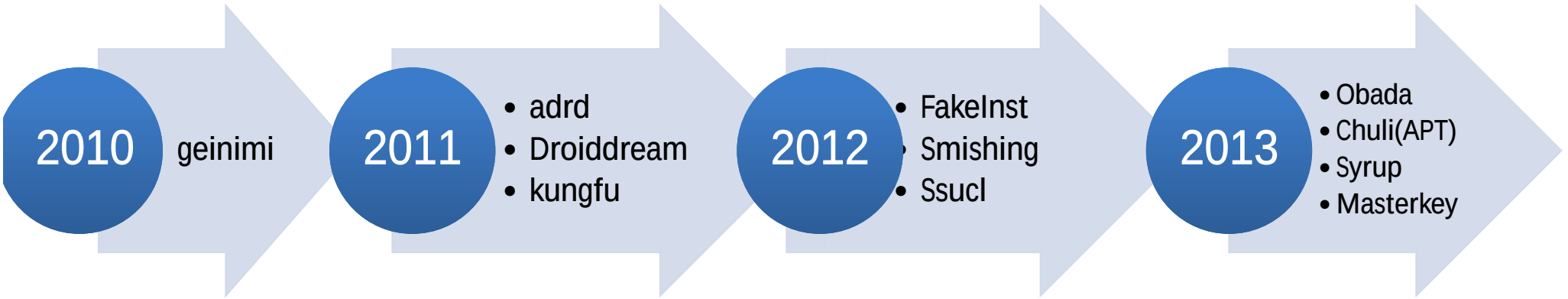


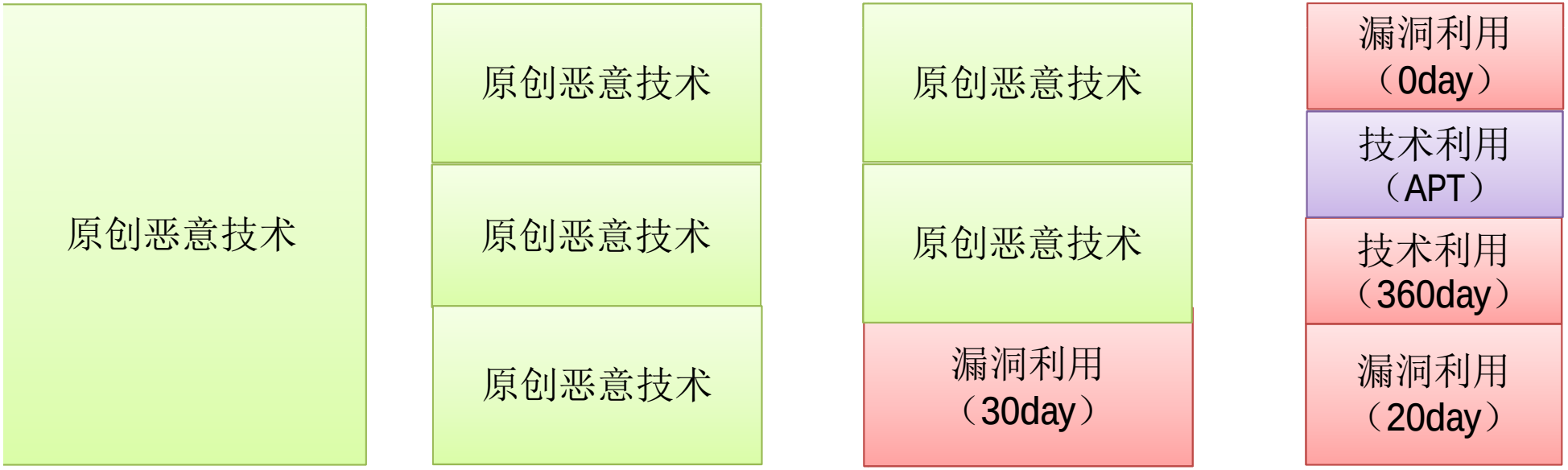


2014年Q1新家族分布图



010~2013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

SA 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**

SA 公司盘点

Application

- **Remotium**

Antivirus&Protection

- Lookout， Bluepoint

BYOD/MDM

- AirWatch， MobileIron， Mocana， Zenprise

Service

- Appthority， PinDrop， Veracode

Solution

- PANW,FireEye,.....

境外移动安全团队

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

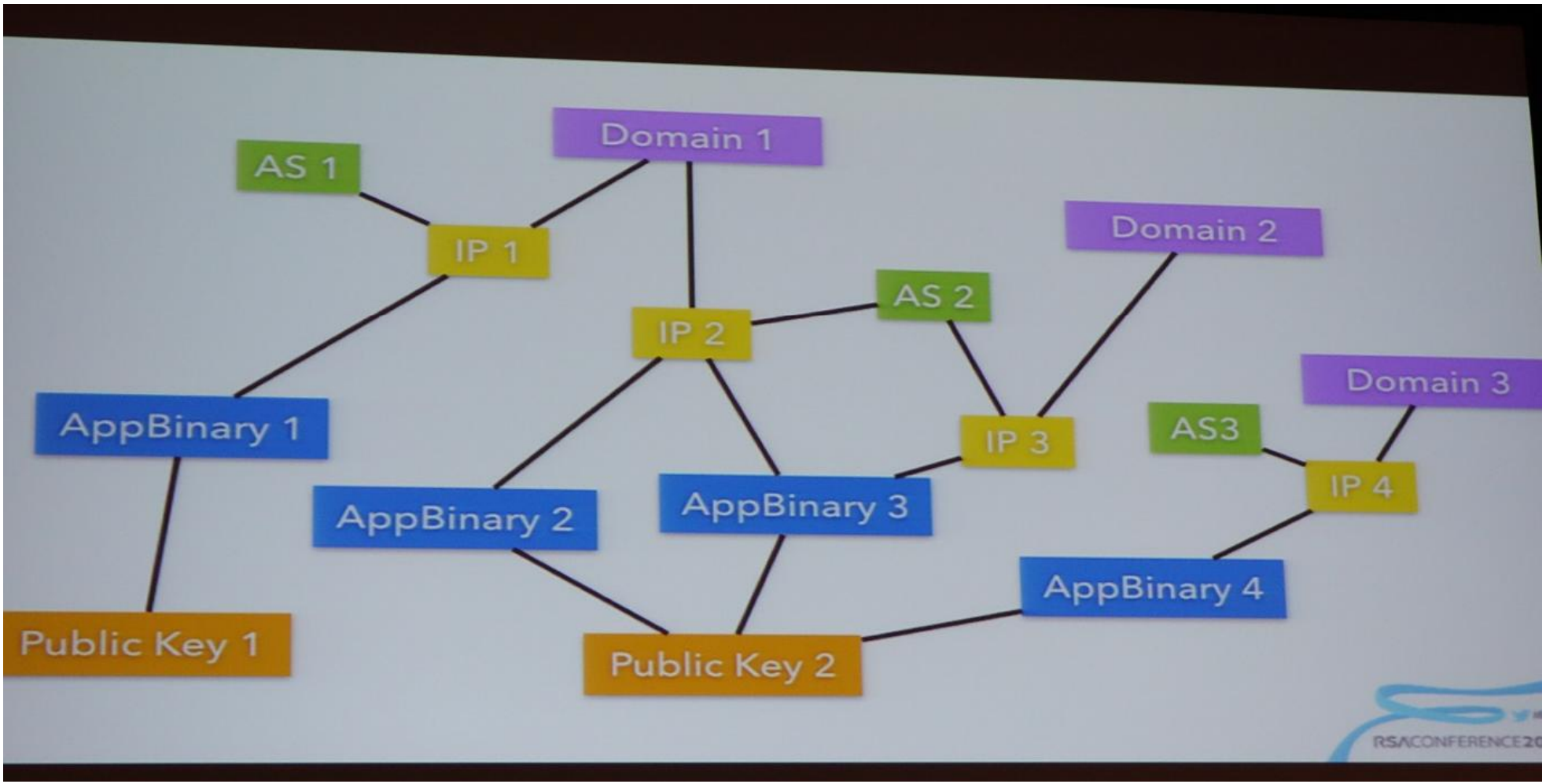
蒋旭宪老师研究团队

- **2011**，**2012**多次首发多个**Android**恶意代码家族和漏洞

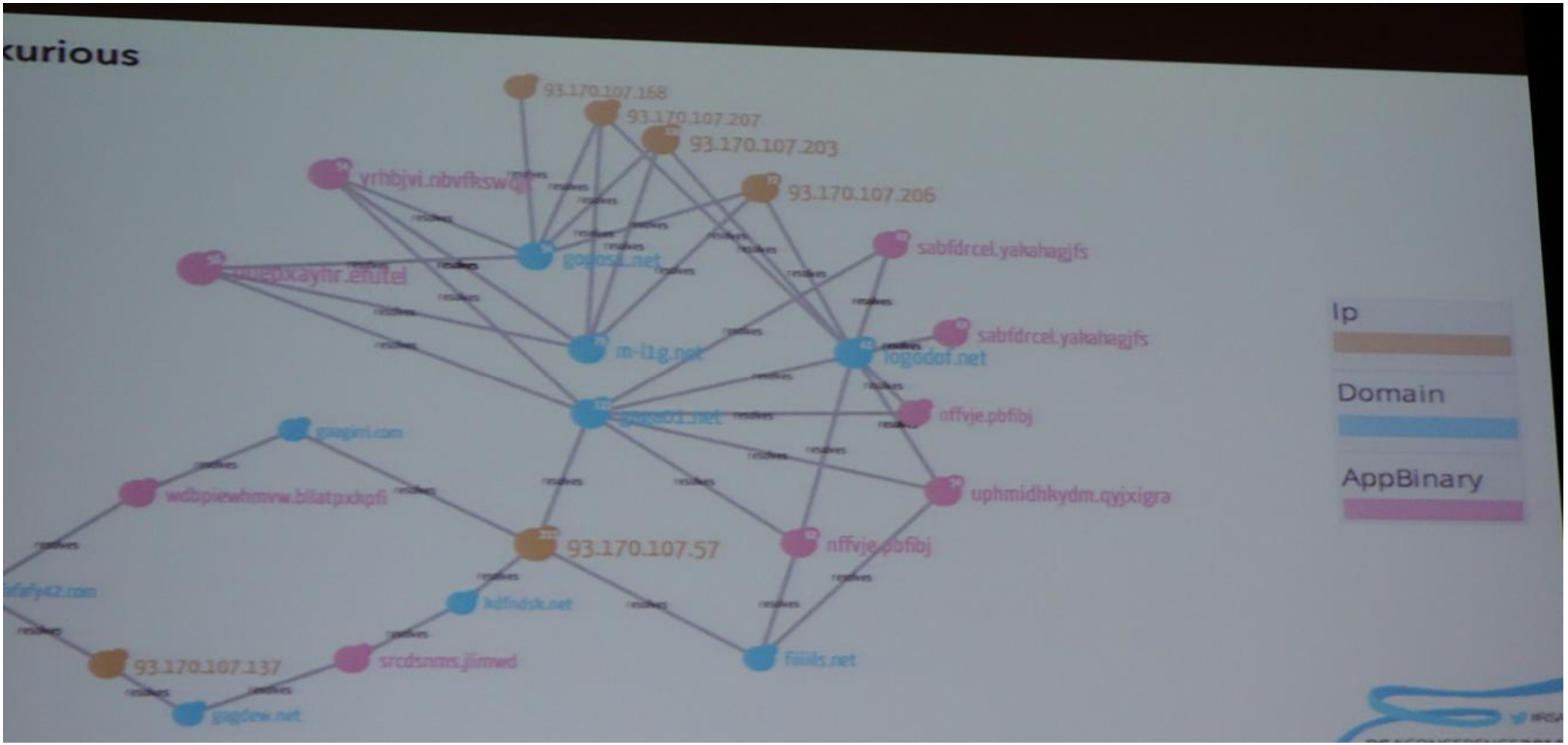
Start-up&Other

- **Appthority**
- **Veracode**
- **Trustlook**，**VisualThreat**
- **Zimperium**，**lacoon**

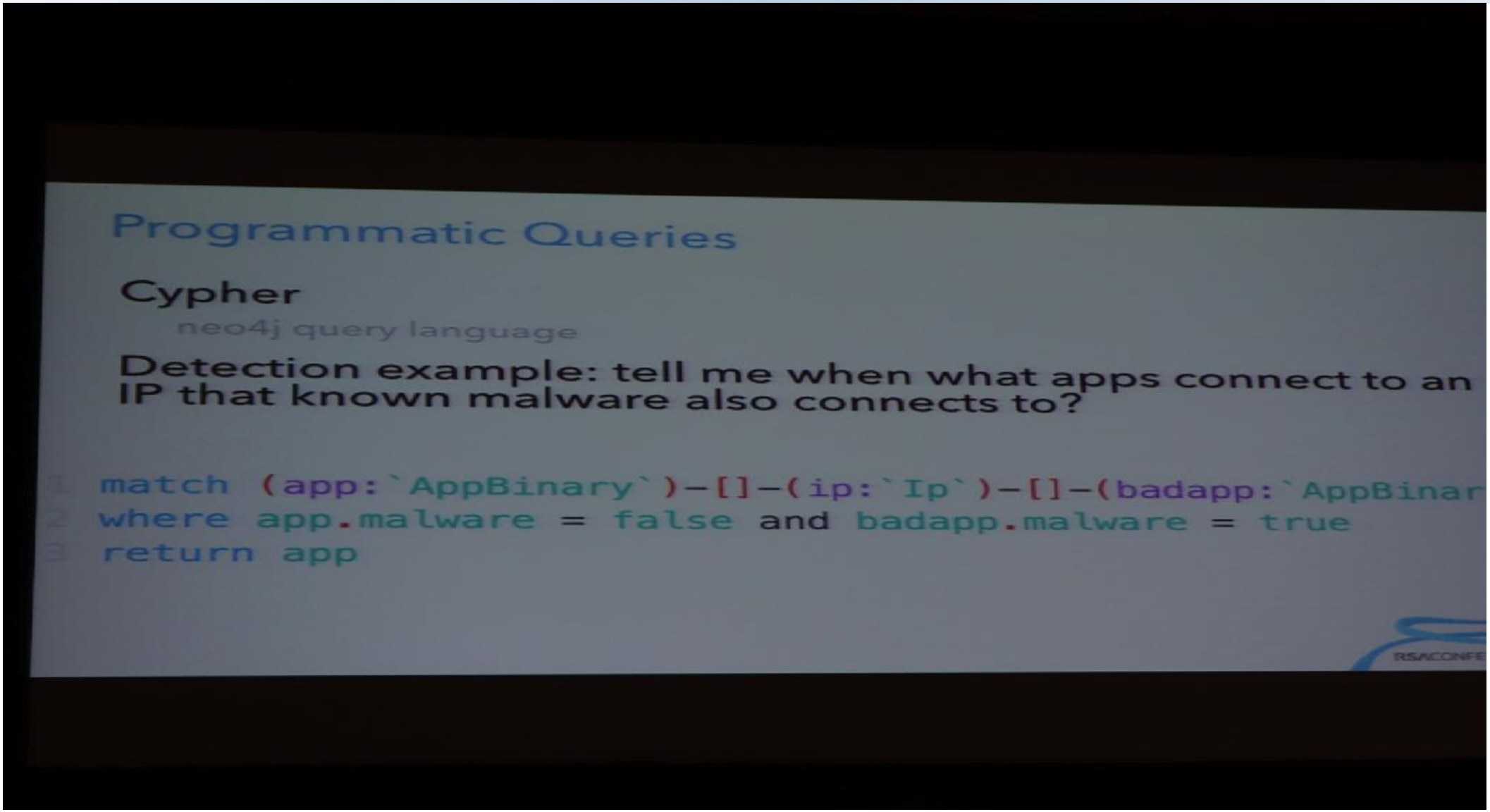
ookout的可视化分析



ookout的可视化分析



ookout的可视化分析



lobileIron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-hou apps, App Store apps, and web apps:

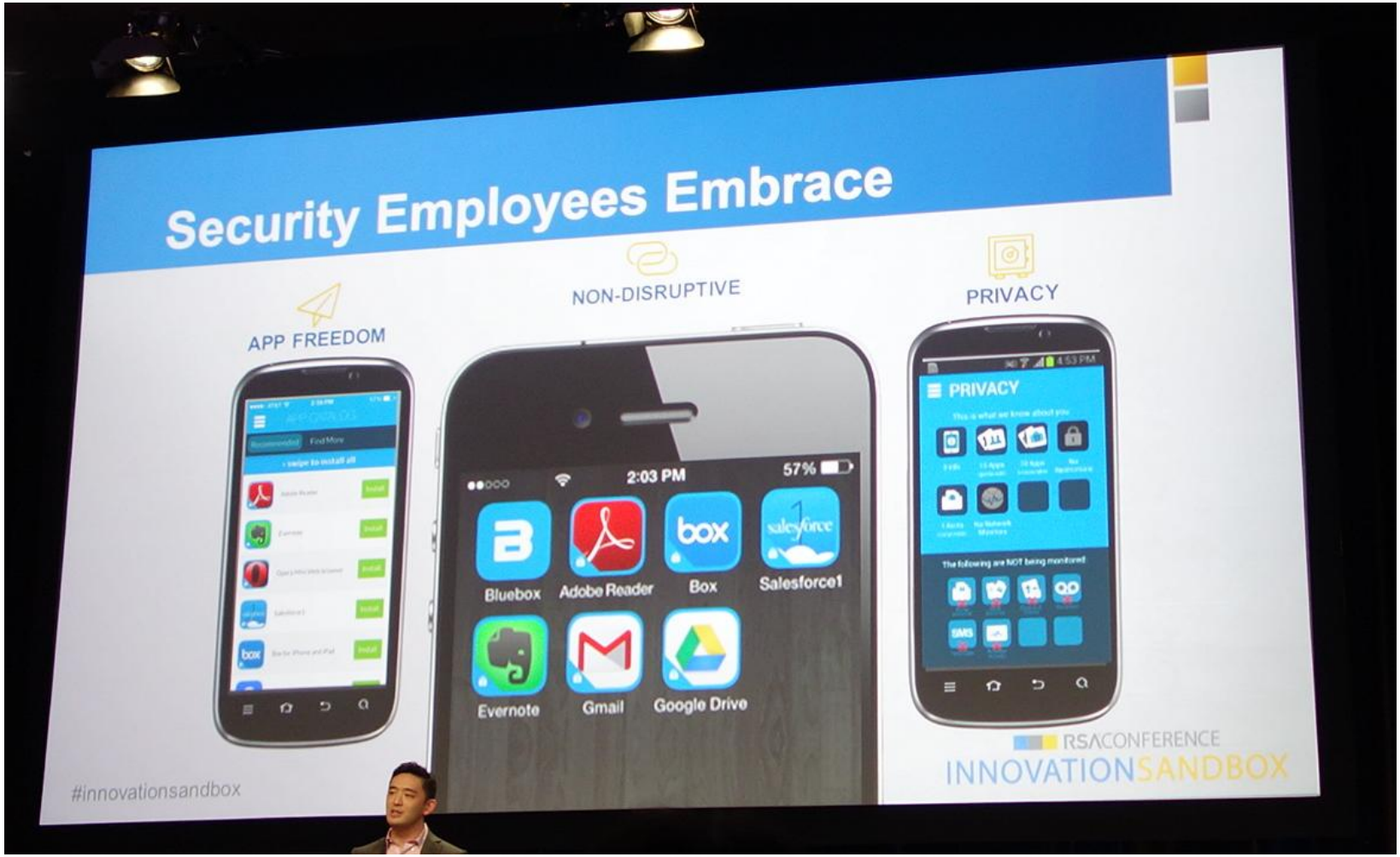
- Secure, identity-based delivery of in-house and App Store apps throu *Apps@Work* private app storefront
- Distribution and silent install of HTML apps as Web Clips
- Selective wipe of business apps and apps data on the device
- Blacklist/whitelist of apps to protect against inappropriate access or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

locana的技术特点

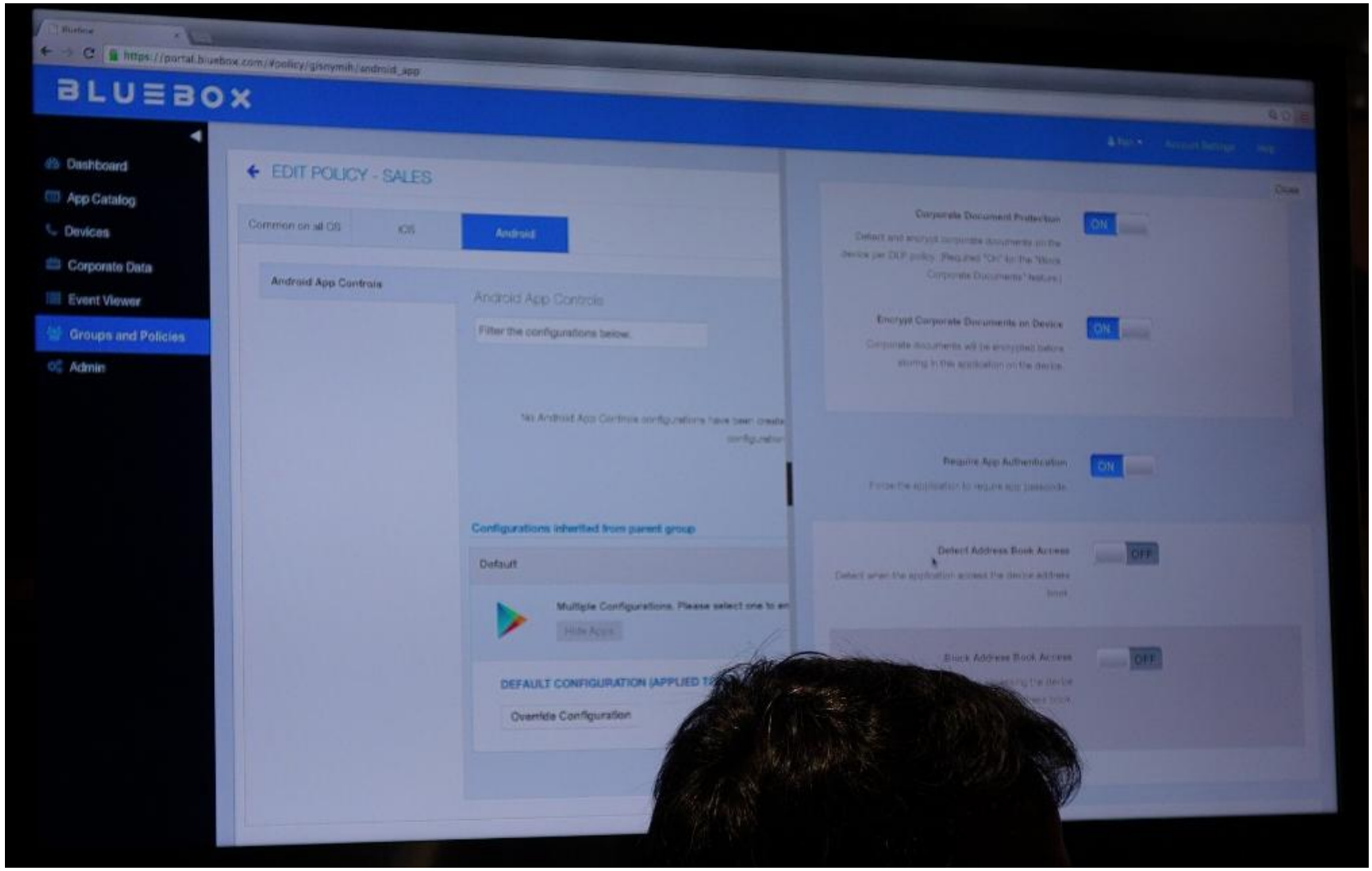
控制通路

透明便利

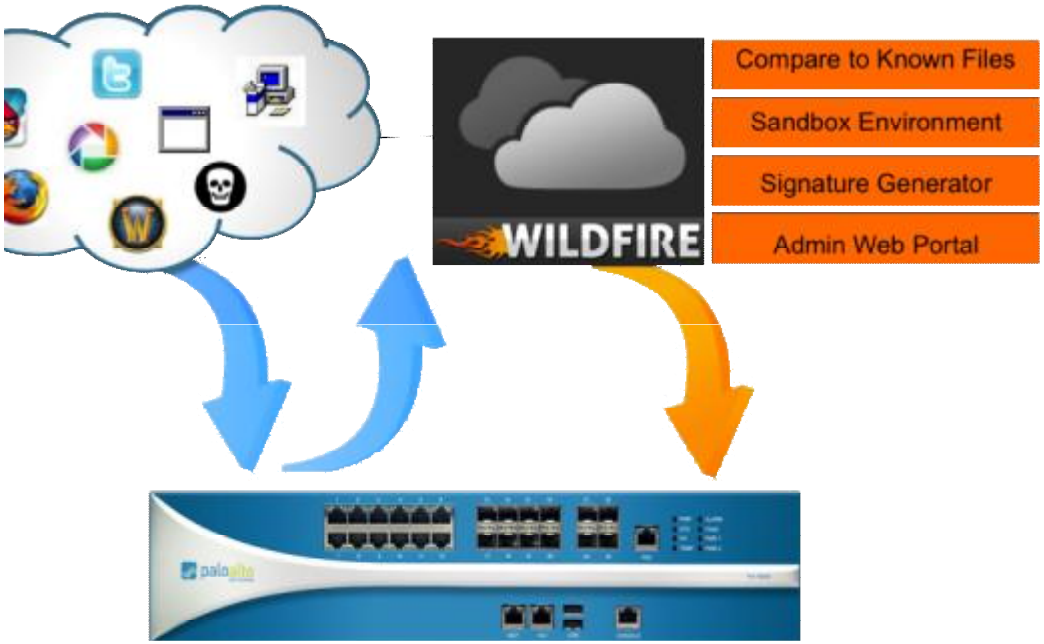
luebox的安全Context Container技术



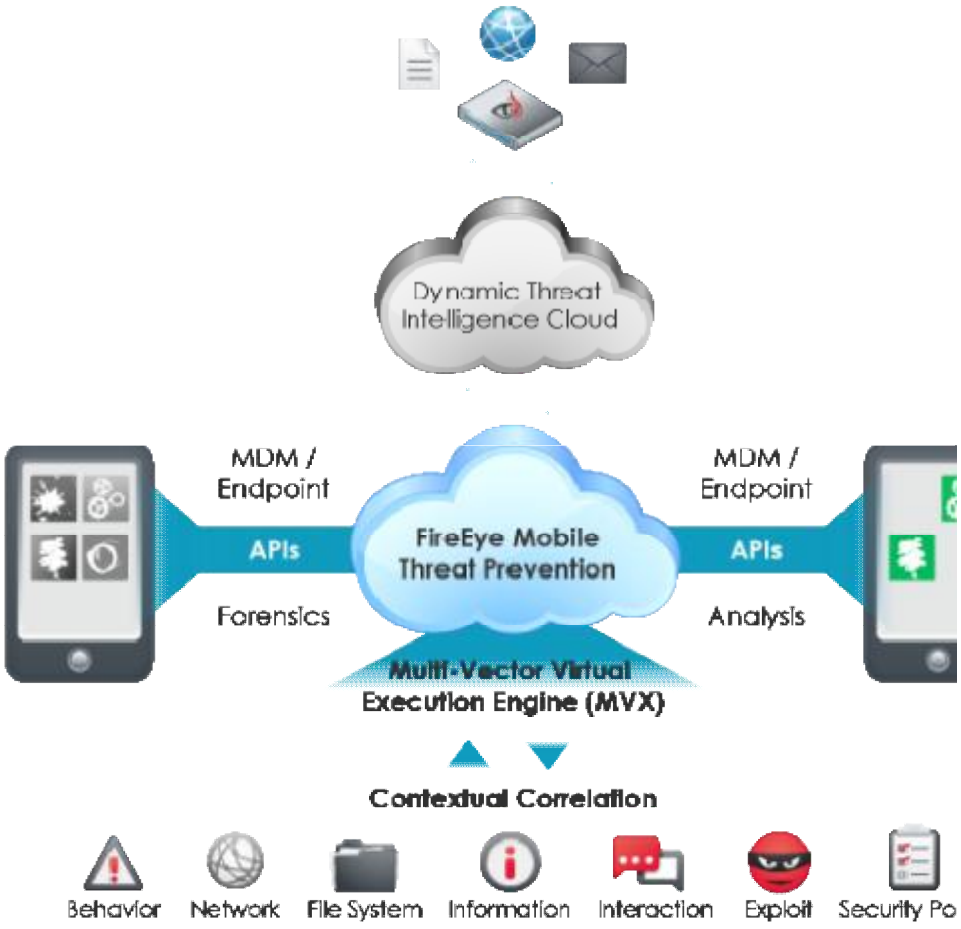
luebox的安全Context Container技术



reEye&PANW



WildFire



MobileThreatPrevention

tart-up/Other

应用安全风险管理

Mobile APT

Analysis Service

Audit Service

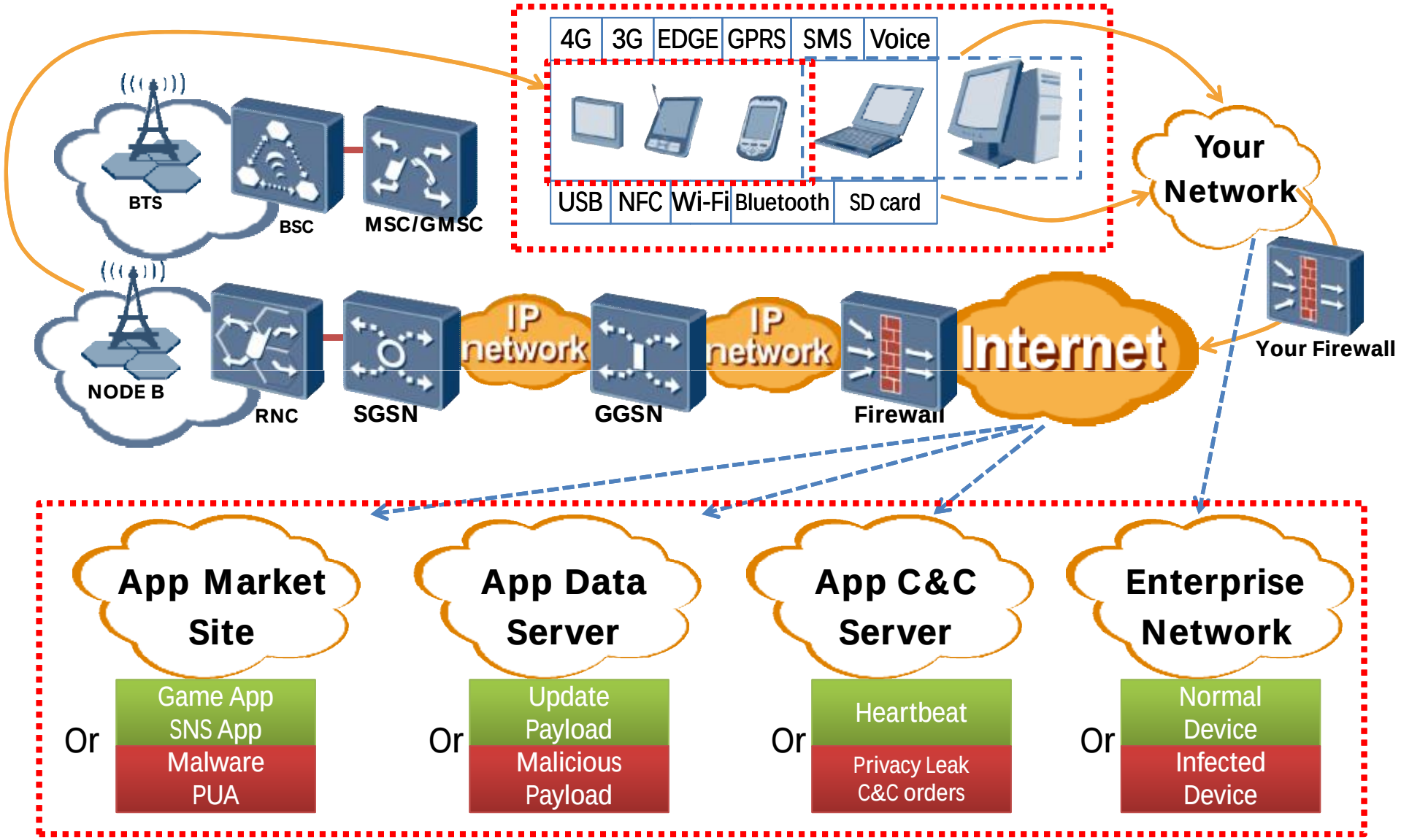
Mobile IPS

Behavior-ed Based

安全需求和技术的角度

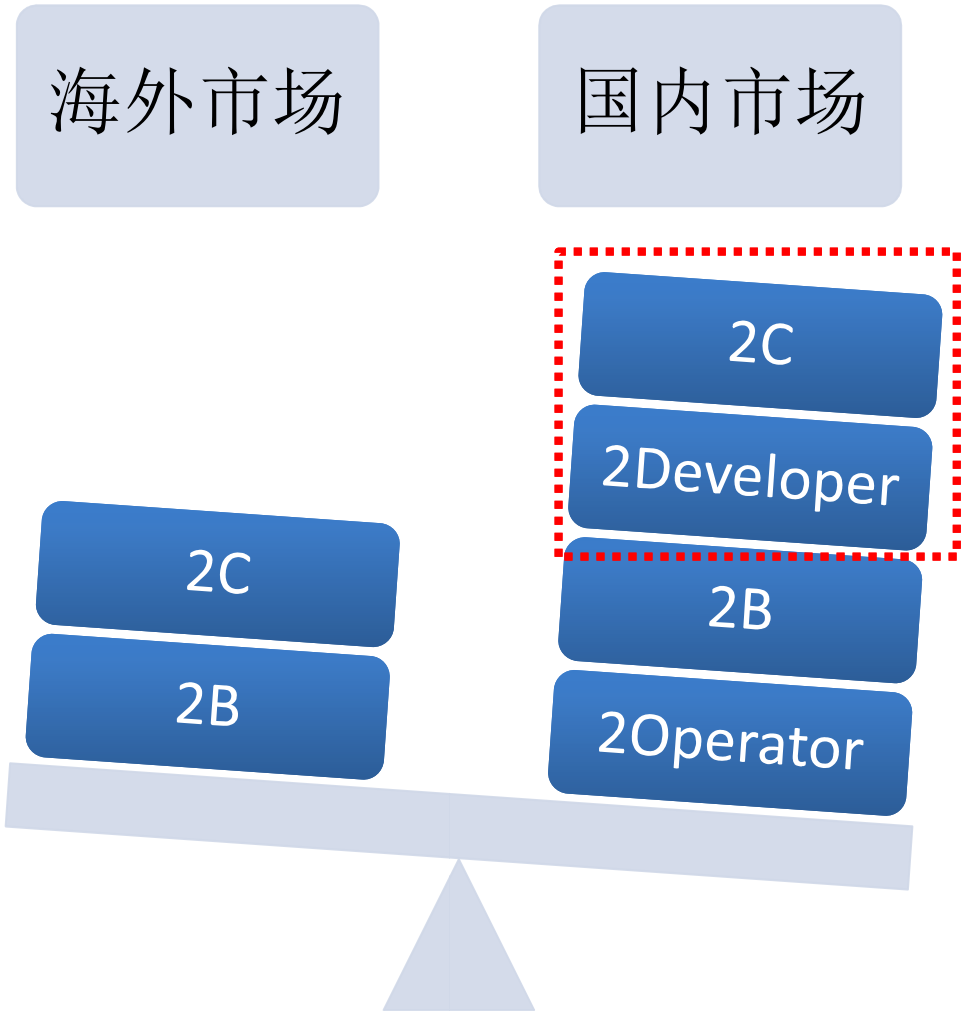
安全需求和技术在中国和海外差异巨大

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

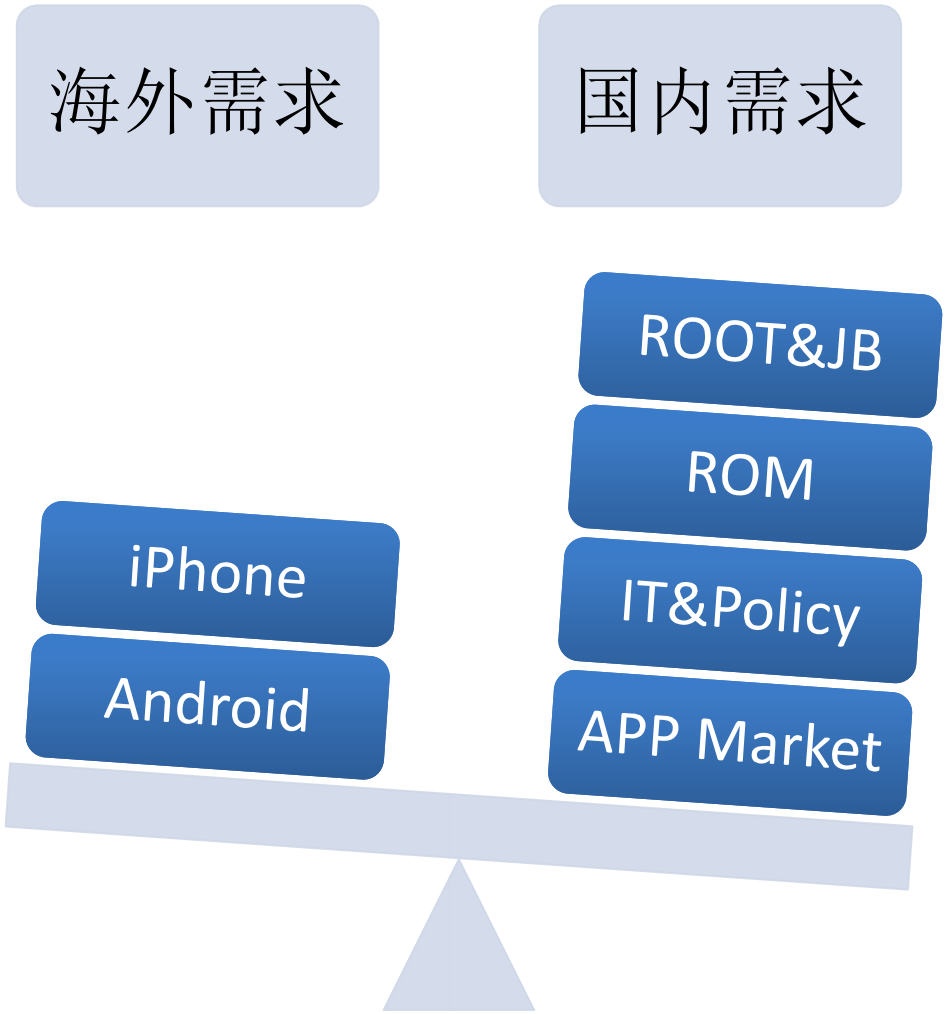
企业级安全为最大市场和需求
个人安全主要被传统PC安全厂商重新划分
技术创新一般，但商业思路成熟



- 个人安全是最大的市场和竞争，安全全面走向范安全
- 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

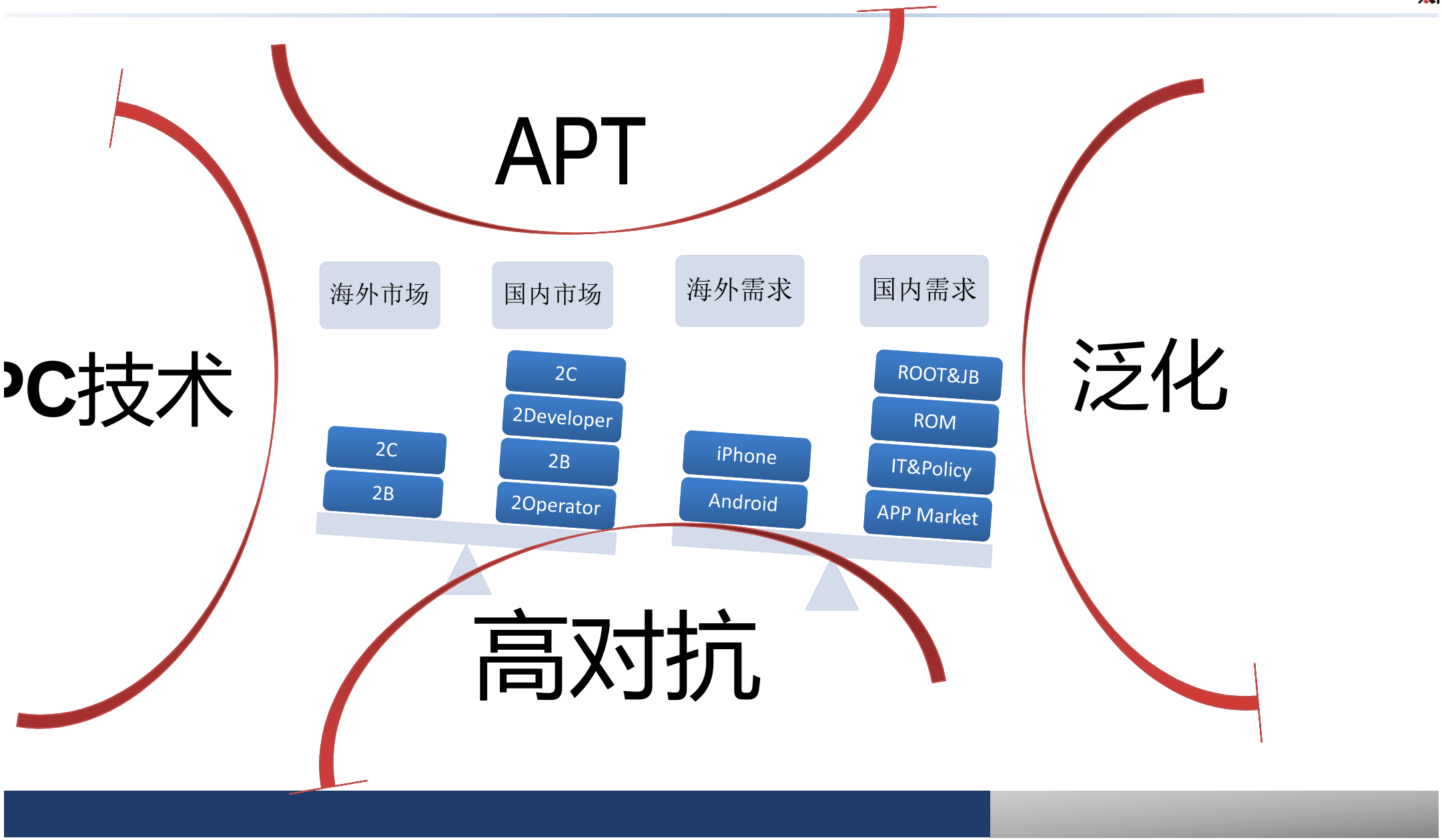
海外和国内的技术需求差异

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
- 行业策略和企业治理，版权保护
- 应用分发渠道发达

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