美国信息安全产业结构与技术发展方向解析

安天实验室 江海客

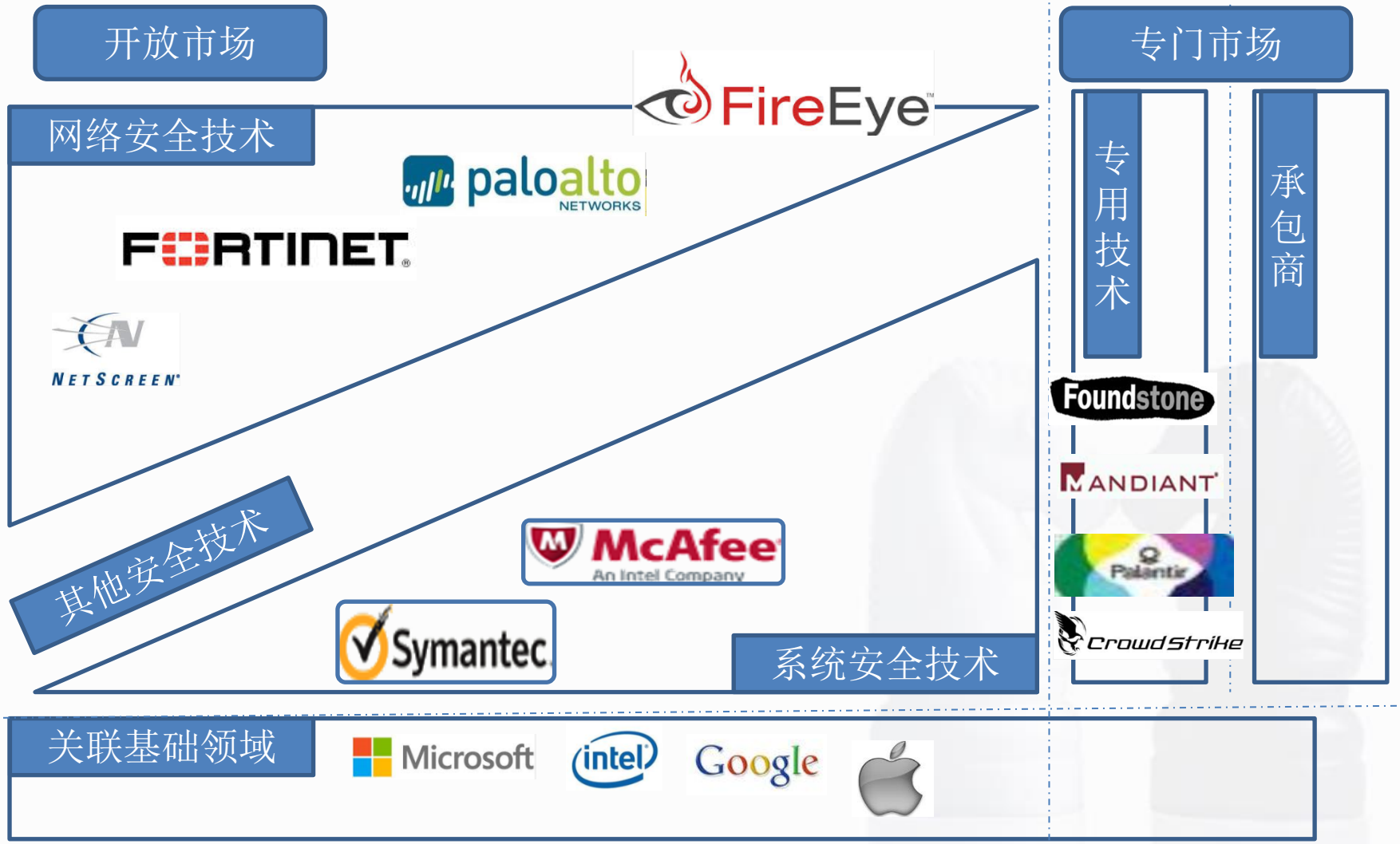
2014.1.16

汇报提纲

- 美国信息安全产业**总体格局透视**
- 硅谷安全企业**创新迭代**与**方法论分析**
- **技术热点分析**

美国信息安全产业总体格局透视

用关系透视格局


开放市场
专门市场
网络安全技术
FireEye
paloalto NETWORKS
FORTINET
NETSCREEN
专用技术
承包商
美国政府
Foundstone
MANDIANT
Palantir
CrowdStrike
其他安全技术
McAfee An Intel Company
Symantec
系统安全技术
关联基础领域
Microsoft
intel
Google

信息寡头——千亿美金公司

Company Name	Country	Sales（单位：乙美元）	Profits（单位：亿美元）	Assets（单位：亿美元）	Market Value（单位：亿美元）	领域
Apple	United States	1647	417	1961	4166	计算机硬件
Google	United States	502	107	938	2684	计算机服务
IBM	United States	1045	166	1192	2395	计算机服务
Microsoft	United States	729	155	1287	2348	软件&程序
AT&T	United States	1274	73	2723	2001	电信服务
Oracle	United States	371	106	794	1720	软件&程序
Verizon Communications	United States	1158	9	2252	1373	电信服务
Cisco	United States	473	93	964	1169	通信设备
Qualcomm	United States	205	66	448	1116	半导体
Intel	United States	533	110	844	1057	半导体

传统巨头——能力枢纽

1982.3.1创办

21500员工（2013）

2012财年销售额67亿美金

个人用户收入21亿，企业收入46.3亿

1987年创办

10000余员工（2011）

2010年其销售额约未20亿美金

2011.8.19被Intel以76.8亿美金收购

1988年创办

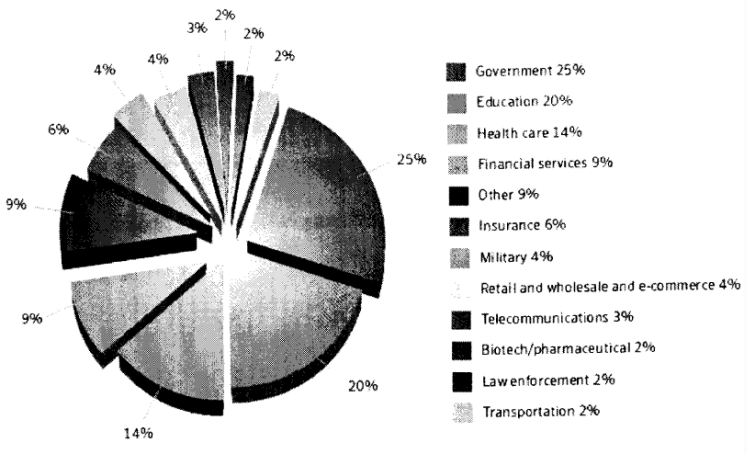
5137名员工（2012）

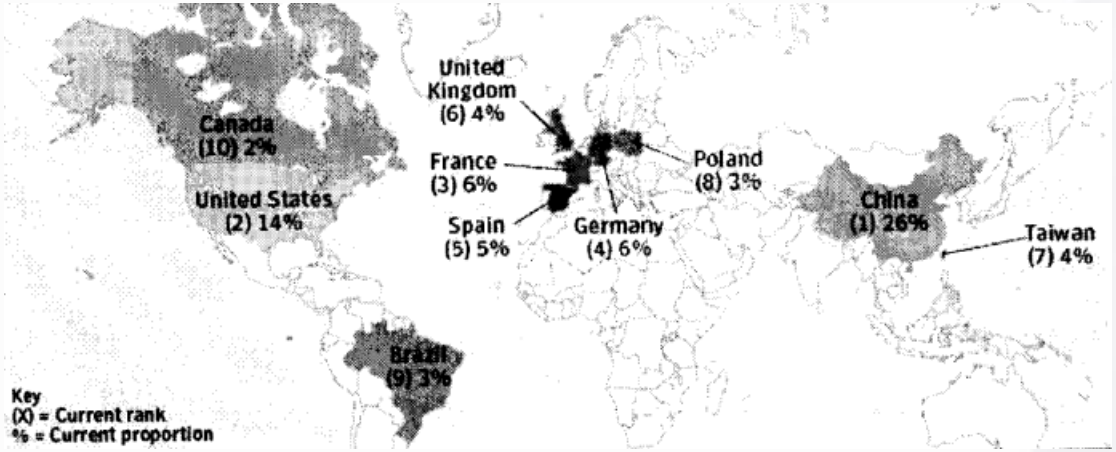
12亿美金（2011）

企业：62%，

个人：38%

传统安全巨头对美国国家安全的助力





图片因自**赛门铁克2006年上半年互联网安全威胁报告**

变局：大并购时代——价值启示录

大并购的时代

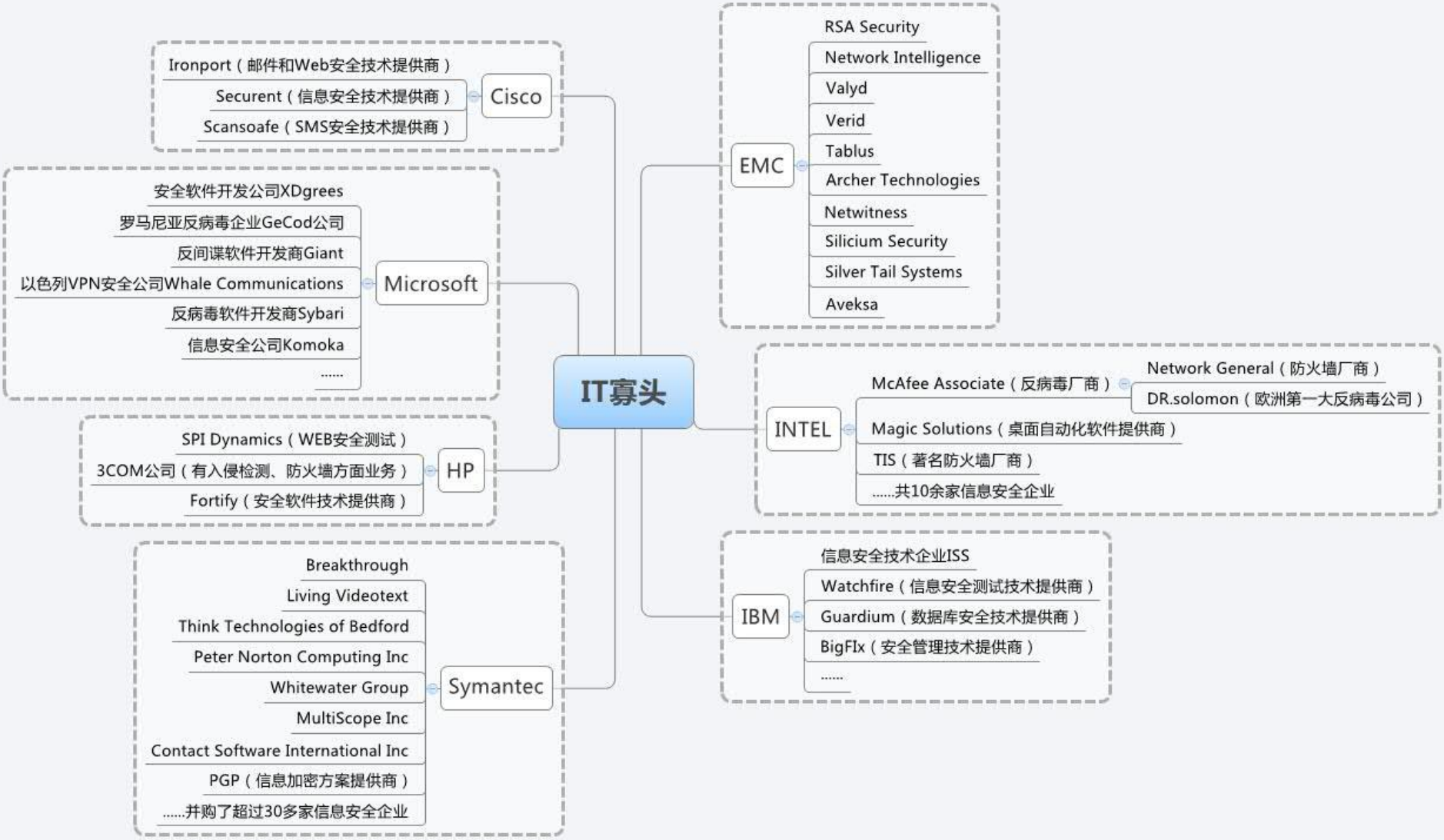
时间	收购方	被收购方	交易金额	被收购方情况和其他备注
2010.8	Intel	McAfee	76.8亿美金	反病毒业巨头企业
2012.8	Cisco	NDS	50亿美金	视频内容安全解决方案
2004.2	Juniper	Netscreen	35亿美金	硬件防火墙领导厂商
2013.6	Cisco	sourcefire	27亿美金	开源安全代表厂商
2012.7	Dell	Quest Software	24亿美金	企业软件厂商
2010.9.13	HP	ArcSight	15亿美金	日志分析厂商
2006.8	IBM	ISS	13亿美金	著名安全扫描服务厂商
2010.8	Symantec	VeriSign	12.8亿美金	著名电子认证厂商
2014.1	Fireeye	Mandiant	10亿美金	著名APT分析厂商

2011~2013 狂涛汹涌

2012～2013 与网络安全相关的主要并购案

收购方	被收购方	并购原因	Terms 金额
Acronis	GroupLogic	Consolidation move to ensure secure enterprise file access, sharing and syncing.	Undisclosed
Apple	AuthenTec	Increase market share and add security technology to its iPhones as mobile payments become more prominent.	$356 million
Cisco	Lightwire	Will allow Cisco to deliver high-speed networks with the next generation of optical connectivity.	$271 million
	NDS	Video software and content security solution.	$5 billion
	Truviso	Provides network data analysis and reporting software technology.	Undisclosed
		Will help Cisco build distributed cloud infrastructure that ties into its own Open	

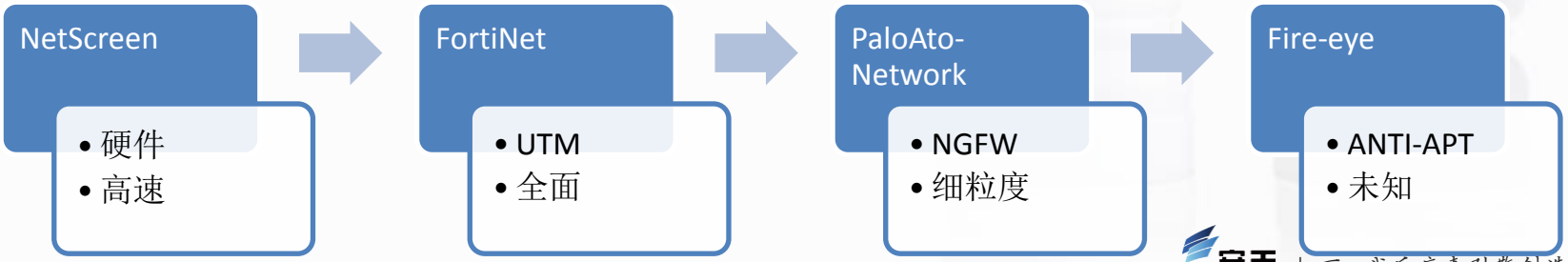
跨行业寡头体系的形成


IT寡头
Cisco
Ironport（邮件和Web安全技术提供商）
Securent（信息安全技术提供商）
Scansoafe（SMS安全技术提供商）
EMC
RSA Security
Network Intelligence
Valyd
Verid
Tablus
Archer Technologies
Netwitness
Silicium Security
Silver Tail Systems
Aveksa
Microsoft
安全软件开发公司XDgrees
罗马尼亚反病毒企业GeCod公司
反间谍软件开发商Giant
以色列VPN安全公司Whale Communications
反病毒软件开发商Sybari
信息安全公司Komoka
.....
INTEL
McAfee Associate（反病毒厂商）
Network General（防火墙厂商）
DR.solomon（欧洲第一大反病毒公司）
Magic Solutions（桌面自动化软件提供商）
TIS（著名防火墙厂商）
.....共10余家信息安全企业
HP
SPI Dynamics（WEB安全测试）
3COM公司（有入侵检测、防火墙方面业务）
Fortify（安全软件技术提供商）
IBM
信息安全技术企业ISS
Watchfire（信息安全测试技术提供商）
Guardium（数据库安全技术提供商）
BigFIx（安全管理技术提供商）
.....
Symantec
Breakthrough
Living Videotext
Think Technologies of Bedford
Peter Norton Computing Inc
Whitewater Group
MultiScope Inc
Contact Software International Inc
PGP（信息加密方案提供商）
.....并购了超过30多家信息安全企业

硅谷安全企业创新迭代与方法论分析

主流安全网关（防火墙）企业的创新迭代

厂商	Netscreen	Fortinet	Paloalto Network	Fireeye
创建时间	1997.12	2000.12	2005	2004.1.1
上市时间	2001.12.12	2009.11.19	2012.7.27	2013.9.22
核心概念	硬件防火墙	UTM（统一威胁管理）	NG-FW（下一代防火墙）	Advanced Persistent Threat (APT) Attack & Zero-Day Protection
概念提出时间	1999.9	2004.2	2007.6.24	2011
主要产业背景	信息高速公路建设，网络带宽迅速增长。	网络应用蓬勃发展	网络客户端、社交网络等新型态，带宽进一步增长	国家和政经集团间的相互攻击入侵
主要应对威胁	新的流量压力	邮件病毒、垃圾邮件、	SNS威胁、小众协议、僵尸网络	APT
核心技术方法	ASIC专用芯片	流还原检测、与传统文件病毒检测技术结合	精细协议解析 身份ID识别 可视化 基于多核体制和专有实现的高性能	沙箱前置 污点监测



Netscreen

奋发奠基

毛宇明加入 1997.12

红衫资本 370万美金投资 1998.6

童建、罗东平、韦文 1998

艰难成长

1080万美金融资 1999.7

谢青离开创办飞塔 1999.9

第一代GigaScreen ASIC发布

员工数45人

NetScreen-1000，第一款千兆防火墙发布

曲折前行

3600万美金融资 2000.7.25

员工数180人，总卖出设备为15410台

GigaScreen II发布，实现了Fast Path与Slow Path的分离

发布了NS5200、NS5400以及后来的ISF2000系列

IPO&被收购之路

员工数332人，研发比例29%，2001.9.30

2001.12.12，高盛带领Nasdaq上市

2004，Juniper用近40亿美金收购Netscreen

Fortinet

从容启航

创建 2000.12

53百万美金融资 2004.2

投资方：DEFTA Partners、橡子园、联想投资、红点投资、智基创投及Meritech Captital Partners 等

产品：Fortigate（UTM）

团队建设

CTO：Michael Xie 谢华CFO：Ken Goldman as Director of Products：Koroush Saraf

CEO:Ken Xie

VP of Product Marketing:Freddy Mangum 2006.1.1

飞速扩张

收购：IPLocks 2008.6.1

数据库安全

收购：Woven Systems 2009.8.20

网络基础设施供应商

趋于稳健

IPO： 2009.11.1

收购：TalkSwitch 2001.4.11

加拿大的公司，创办时间比较早，但发展较慢，主营电话VOIP网关等

收购：XDN/3Crowd Technologies

2012.12.1

基于云计算的服务商

PaloAto-Network

起点高奏

2005年Nir Zuk加入任CTO

2005 Rajiv Batra加入作为工程高级副总裁和创始人

2006.1.1A轮融资千万美金

2006-2013 毛宇明加入

产品隐忍

2007.1.1 Ron Hornbaker加入作为技术顾问

2007.6.24 PA-4000产品正式发布，主打应用可视化及控制特性

2007.6.25 B轮融资1800万美金，Greylock主投

风头正健

2008.4.27 发布PANOS-2.0，增加诸多新的功能特性

2008.6.1Lane Bess加入任CEO

2008.8.8 C轮第一阶段融资2660万美金

2008.12.14 首次在防火墙中集成DLP数据泄漏保护特性

IPO&上市

2012.7.27上市大涨55%，市值约37.6亿美金

2012.11.12 VM-Series、Wildfire、PA-3000，M100发布

2013.5.18 GlobalProtection解决方案支持IOS和Android系统

Fire-eye

强势启航

创办：2004.1.1

研发及战略线灵魂人物Ashar Aziz：Founder, Vice Chairman of the Board, CTO, and Chief Strategy Officer.

潜伏积累

645万美金A轮融资 2005.1.1

1450万美金B轮融资 2006.8.1

1450万美金C轮融资，Juniper、红杉 2008.5.12

Vice President of Engineering and Security Research：Bahman Mahbod 2007.11.13

产品潜伏期 虚拟机技术 2004-2008

渐入佳境

CIA旗下的投资机构in-q-tel正式入场 2009.11.18

Vice President :

Gene Skiba 2009.12.15

Jeffrey C. Williams 2010.2.18

Alexa King as 2011.4.1

Thomas Schaeffer 2012.1.1

Chief Scientist：峰敏老师

Chief Executive Officer :David DeWalt 2012.11.28

D轮融资5000w美金 2013.1.11

产品发展期：mps 2011-2012

万众瞩目

IPO:175百万美金2013.8.2

更新IPO ： 225 百万美金2013.9.9

产品全面云化： CMS(Central Management System,

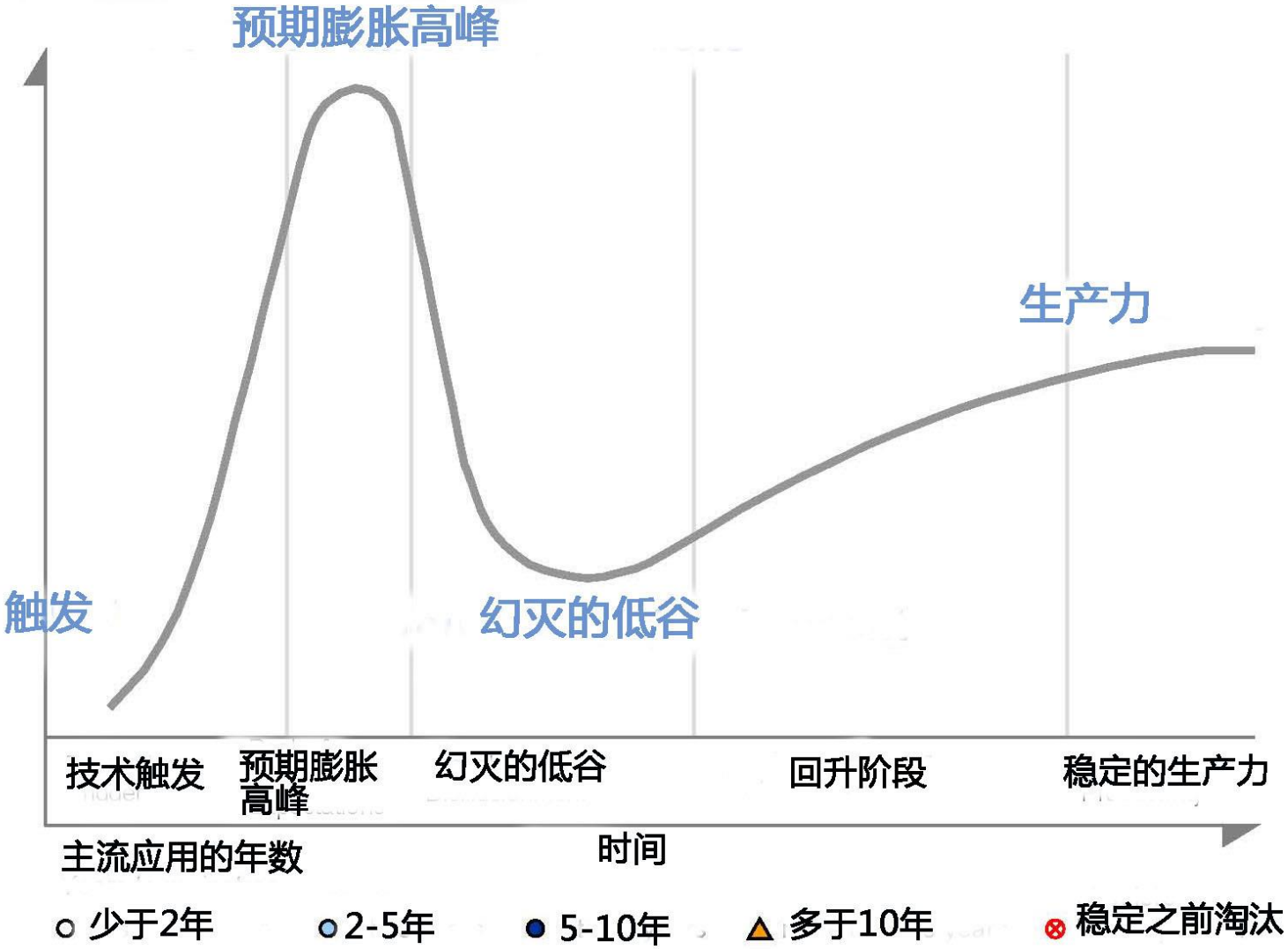
MAS(Malware Analysis System).

2012-2013

硅谷安全企业的特点

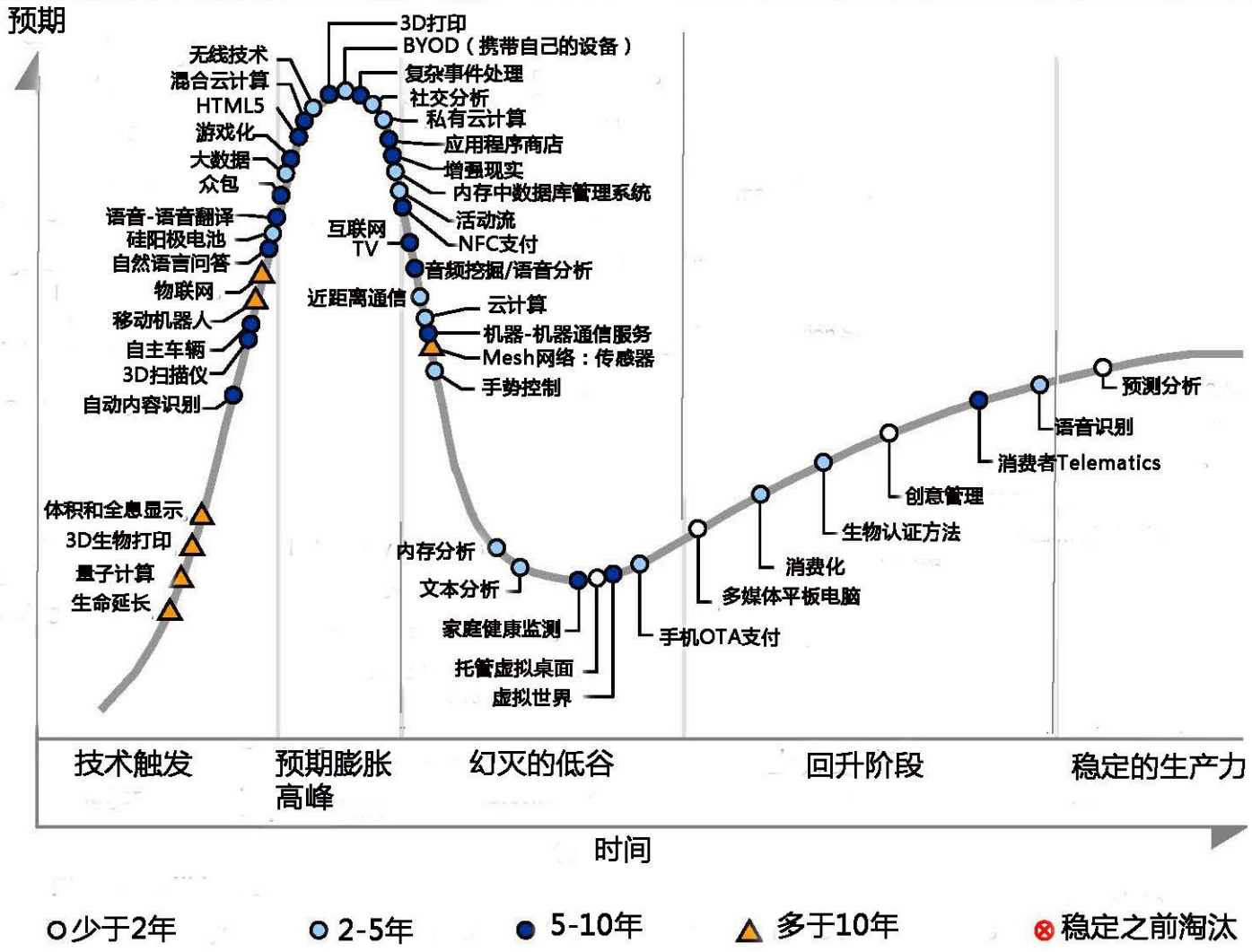
- 不追求面面俱到，不追求大集成者的位置
- 建立自己的企业个性和强点
- 创造自己不可替代的独特价值的话语权
- 寻找个性厂商合作

Gartner 关于技术炒作周期



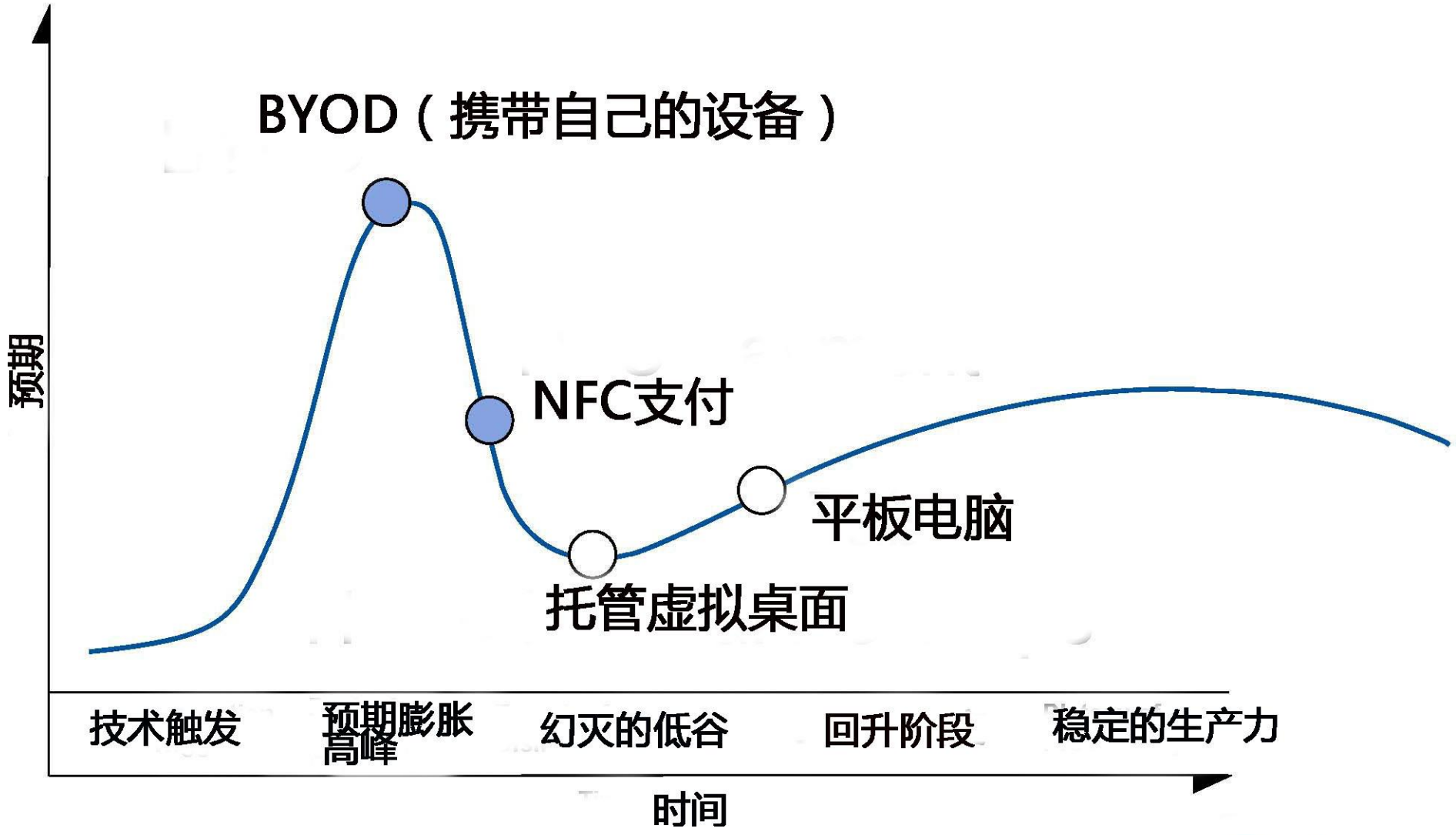
Gartner

安全创新的基础是应用发展



Gartner

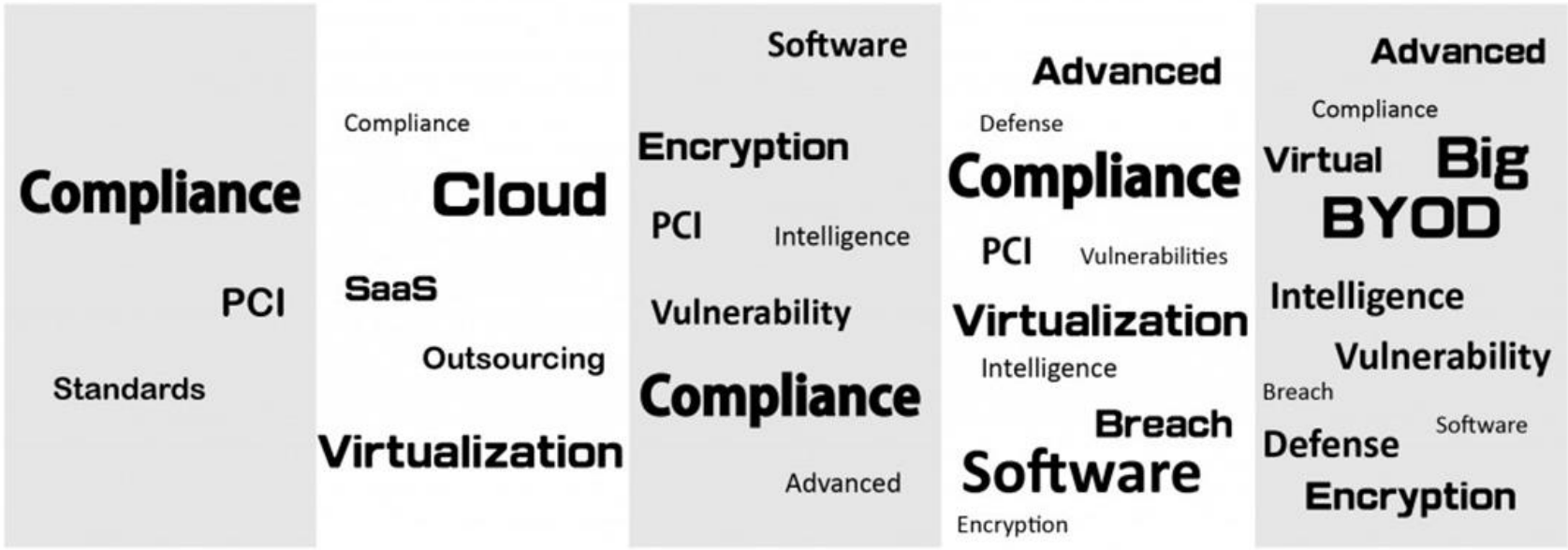
以移动和无线为例



Gartner

攻防与反制APT——技术热点分析

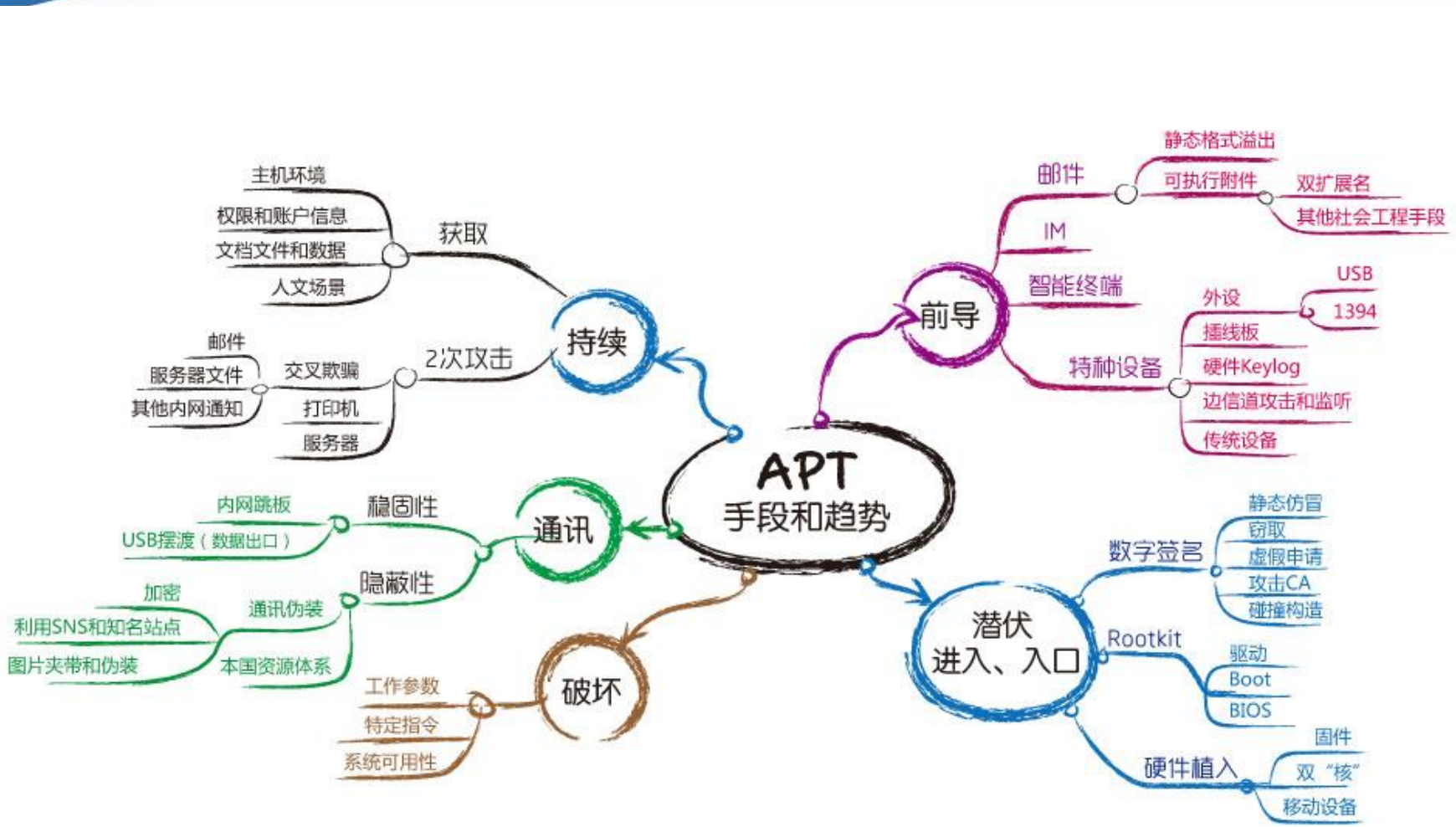
RSA大会行业历年关键词



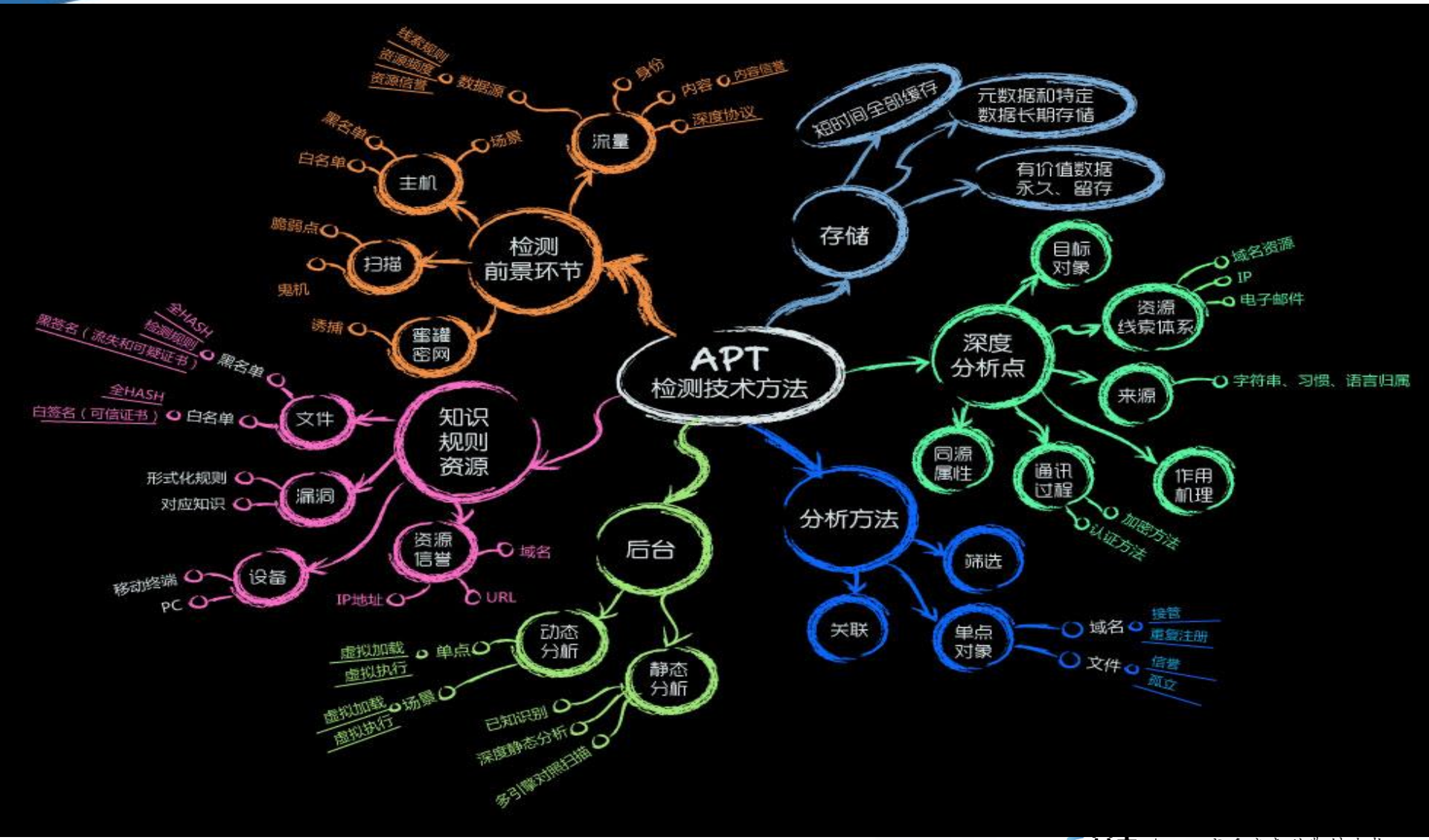
APT识别发现

- 基于虚拟执行的网络侧未知检测
- 基于白名单的终端防护
- 基于IDS的通信发现识别
- 日志数据聚合分析和事件重构
- 事件响应和取证分析

APT手段和趋势


APT
手段和趋势
前导
邮件
静态格式溢出
可执行附件
双扩展名
其他社会工程手段
IM
智能终端
特种设备
外设
USB
1394
插线板
硬件Keylog
边信道攻击和监听
传统设备
持续
获取
主机环境
权限和账户信息
文档文件和数据
人文场景
2次攻击
交叉欺骗
邮件
服务器文件
其他内网通知
打印机
服务器
通讯
稳固性
内网跳板
USB摆渡（数据出口）
隐蔽性
通讯伪装
加密
利用SNS和知名站点
图片夹带和伪装
本国资源体系
潜伏
进入、入口
数字签名
静态仿冒
窃取
虚假申请
攻击CA
碰撞构造
Rootkit
驱动
Boot
BIOS
硬件植入
固件
双“核”
移动设备
破坏
工作参数
特定指令
系统可用性

反APT方法


APT
检测技术方法
检测
前景环节
流量
数据源
线索规则
资源频度
资源信誉
身份
内容
内容信誉
深度协议
主机
黑名单
白名单
场景
扫描
脆弱点
鬼机
蜜罐
密网
诱捕
知识
规则
资源
文件
全HASH
检测规则
黑签名（丢失和可疑证书）
黑名单
全HASH
白签名（可信证书）
白名单
漏洞
形式化规则
对应知识
设备
移动终端
PC
资源
信誉
域名
IP地址
URL
后台
动态
分析
虚拟加载
虚拟执行
单点
虚拟加载
虚拟执行
场景
静态
分析
已知识别
深度静态分析
多引擎对照扫描
存储
短时间全部缓存
元数据和特定
数据长期存储
有价值数据
永久、留存
深度
分析点
目标
对象
域名资源
IP
电子邮件
资源
线索体系
来源
字符串、习惯、语言归属
同源
属性
通讯
过程
加密方法
认证方法
作用
机理
分析方法
筛选
关联
单点
对象
域名
接管
重复注册
文件
信誉
孤立

战略性背景导向

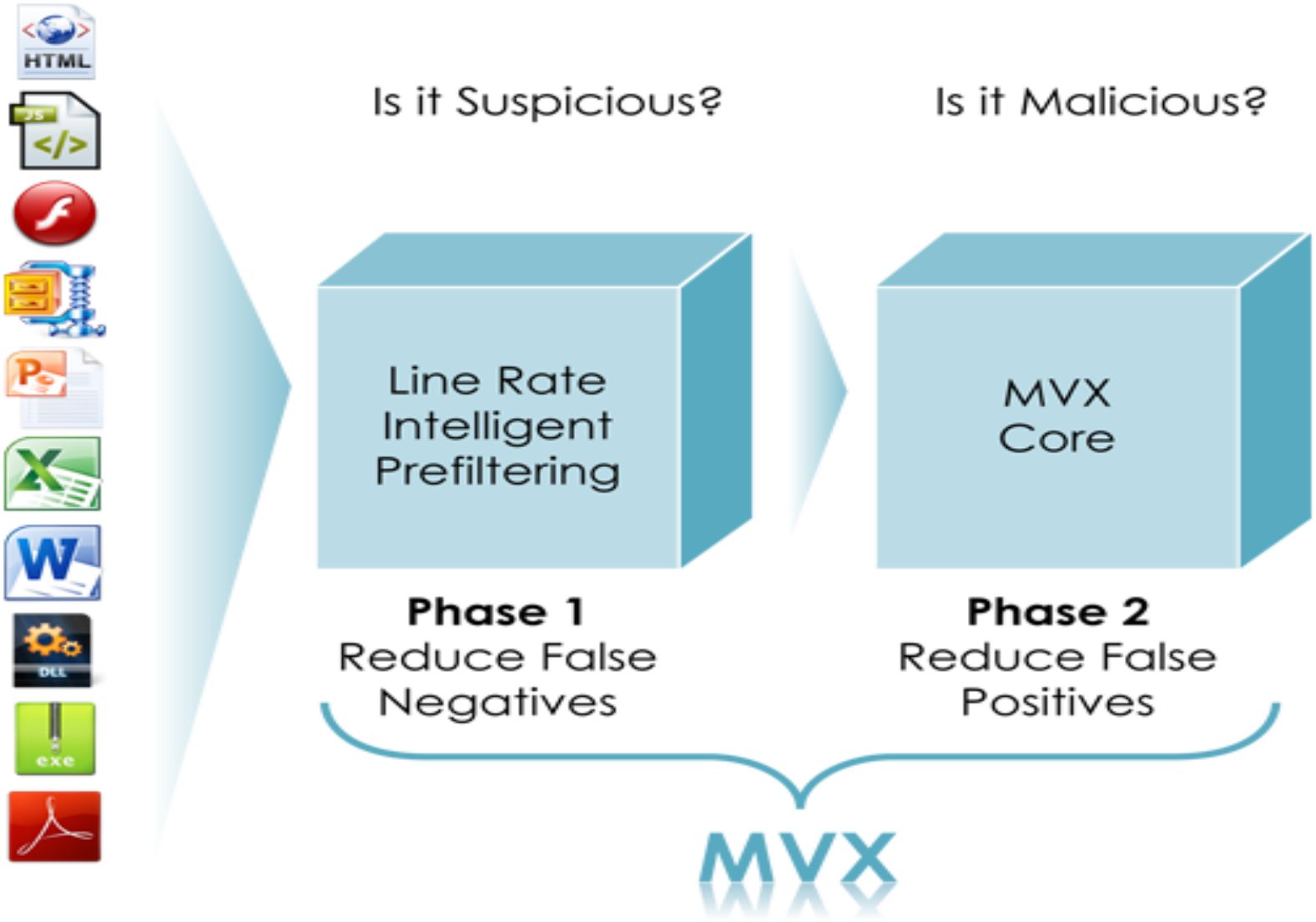
- 不基于特征的未知威胁检测
  - 恶意代码
  - 0day漏洞利用：shellcode、多种格式文件
- 背景： 2013美国国防预算法案932.b
  - 为了克服当前面临的问题和局限性，（下一代网络安全）系统不应依赖于：
  - a. 已知特征机制；
  - b. 需要经常更新的特征机制；
  - c. 需要以数据库形式存储下来的特征机制。

基于虚拟执行的网络侧未知检测

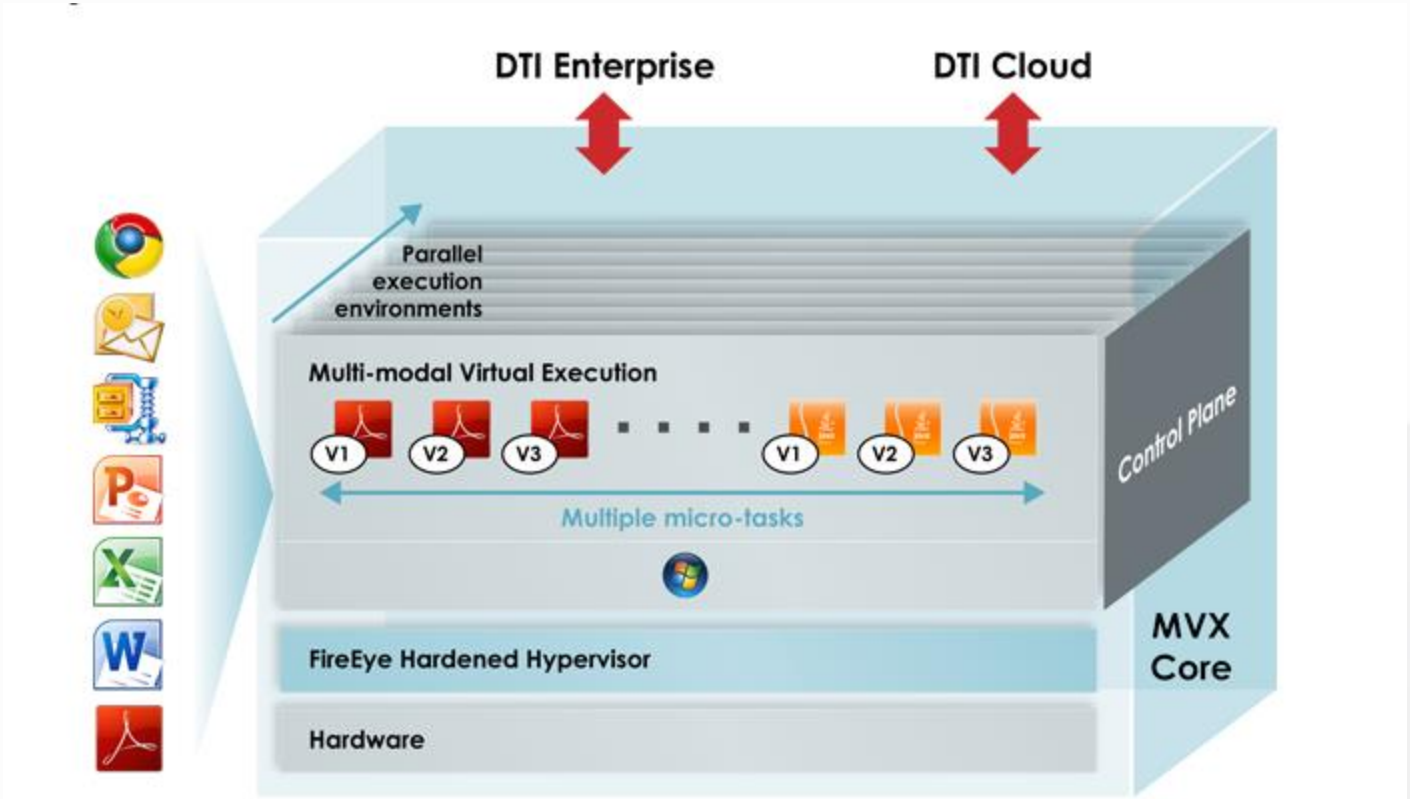
- 典型代表：FireEye
- 在网络设备中对流量数据中异常代码或文件作沙箱虚拟执行，并对内存做污点分析，发现已知和未知的exploit
- Dawn Song等学术研究成果，主持移动的开发。

- 备选代表企业：GFI Software

基于虚拟执行的网络侧未知检测



基于虚拟执行的网络侧未知检测



基于虚拟执行的网络侧未知检测

- FireEye方案
  - MPS(Malware protection System)引擎
  - 支持Web、邮件、文件共享等多种来源数据
  - 专门的MPS硬件运行不同来源数据
  - 除可执行文件外，支持20多种其他文件格式
  - 实时学习恶意代码C&C特征并阻断

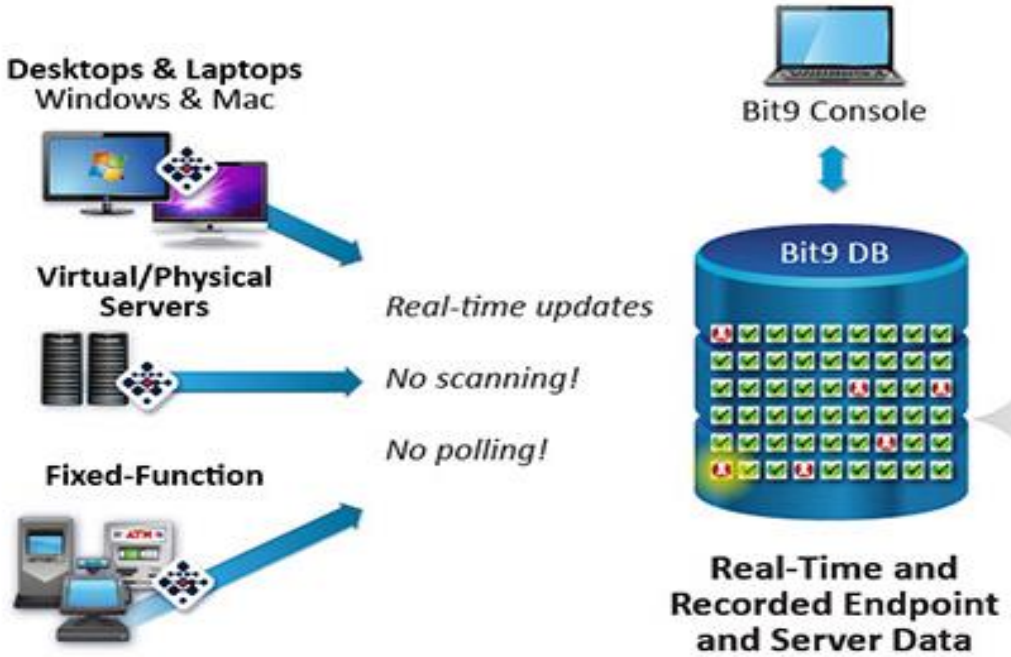
基于白名单的终端防护

- 在终端、服务器中，只允许受信的白名单软件运行
- 典型代表：Bit9
  - 基于策略定义软件的可信性，包括软件开发者和软件分发渠道制定
  - 安全云，提供软件可信度评价服务
  - 实时检测审计，监测、防范、事后审计

基于白名单的终端防护

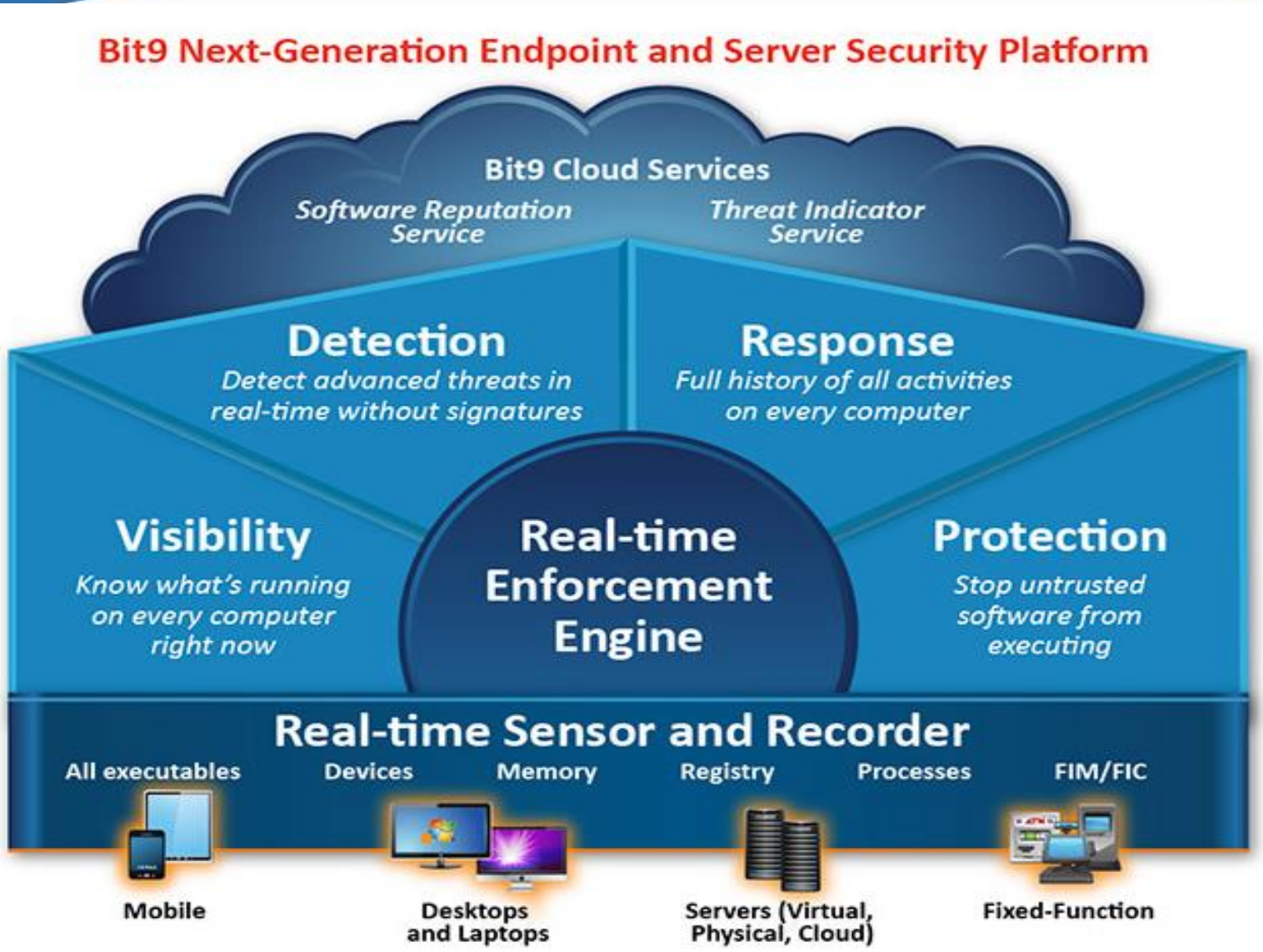
Continuously Monitors and Records Every Computer

Actionable Intelligence
about every endpoint and server



- **Visibility:** ***Instant Intelligence***
  - All new **executables**
  - Did they (attempt to) **run?**
  - What **other files** did they create?
  - **Memory or process violations?**
  - **Configuration** (registry) **changes?**
  - **USB** devices?
  - How many versions of **Java?**
  - **File** changes?
- **Detection:** ***Identify threats***
  - Cloud-delivered **Advanced Threat Indicators** (signature-less)
  - Cloud-delivered file **trust ratings**
- **Response:** ***Prioritize alerts and respond to incidents***
  - **Detailed history** of every machine
  - What happened, when, how, etc.

基于白名单的终端防护


Bit9 Next-Generation Endpoint and Server Security Platform
Bit9 Cloud Services
Software Reputation Service
Threat Indicator Service
Detection
Detect advanced threats in real-time without signatures
Response
Full history of all activities on every computer
Visibility
Know what's running on every computer right now
Real-time Enforcement Engine
Protection
Stop untrusted software from executing
Real-time Sensor and Recorder
All executables
Devices
Memory
Registry
Processes
FIM/FIC
Mobile
Desktops and Laptops
Servers (Virtual, Physical, Cloud)
Fixed-Function

基于白名单的终端防护

- Bit9方案遇到的一个问题
  - 2013年2月，Bit9代码签名证书被盗
  - 至少3家客户发现了由被盗证书签名的恶意代码
  - 它们将被bit9系统认为是可信的软件而可以执行

基于IDS的通信发现识别

- 针对APT中的C&C通信
- 基于格式、特征、模式等，识别流量并予以阻断
- 代表：趋势科技Deep Discovery
  - IDS引擎Inspector，基于全球威胁情报信息检测C&C通道
  - 恶意代码沙箱和分析引擎
  - 全球各个Inspector之间共享情报

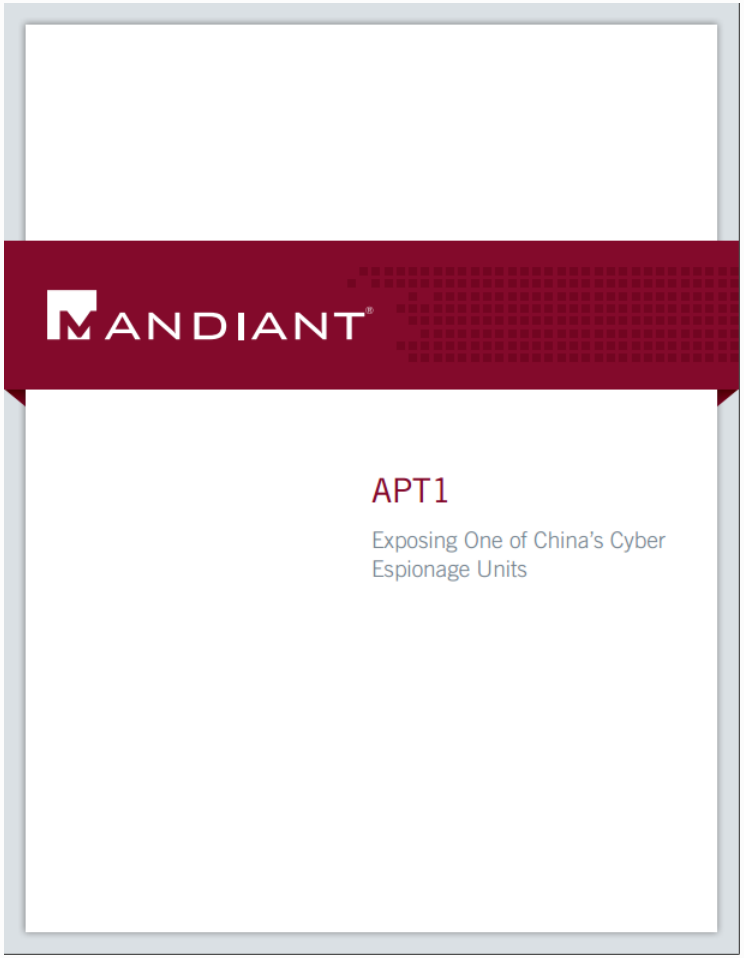
基于IDS的通信发现识别

基于IDS的通信发现识别

Deep Discovery Advisor

基于IDS的通信发现识别

事件响应和取证分析



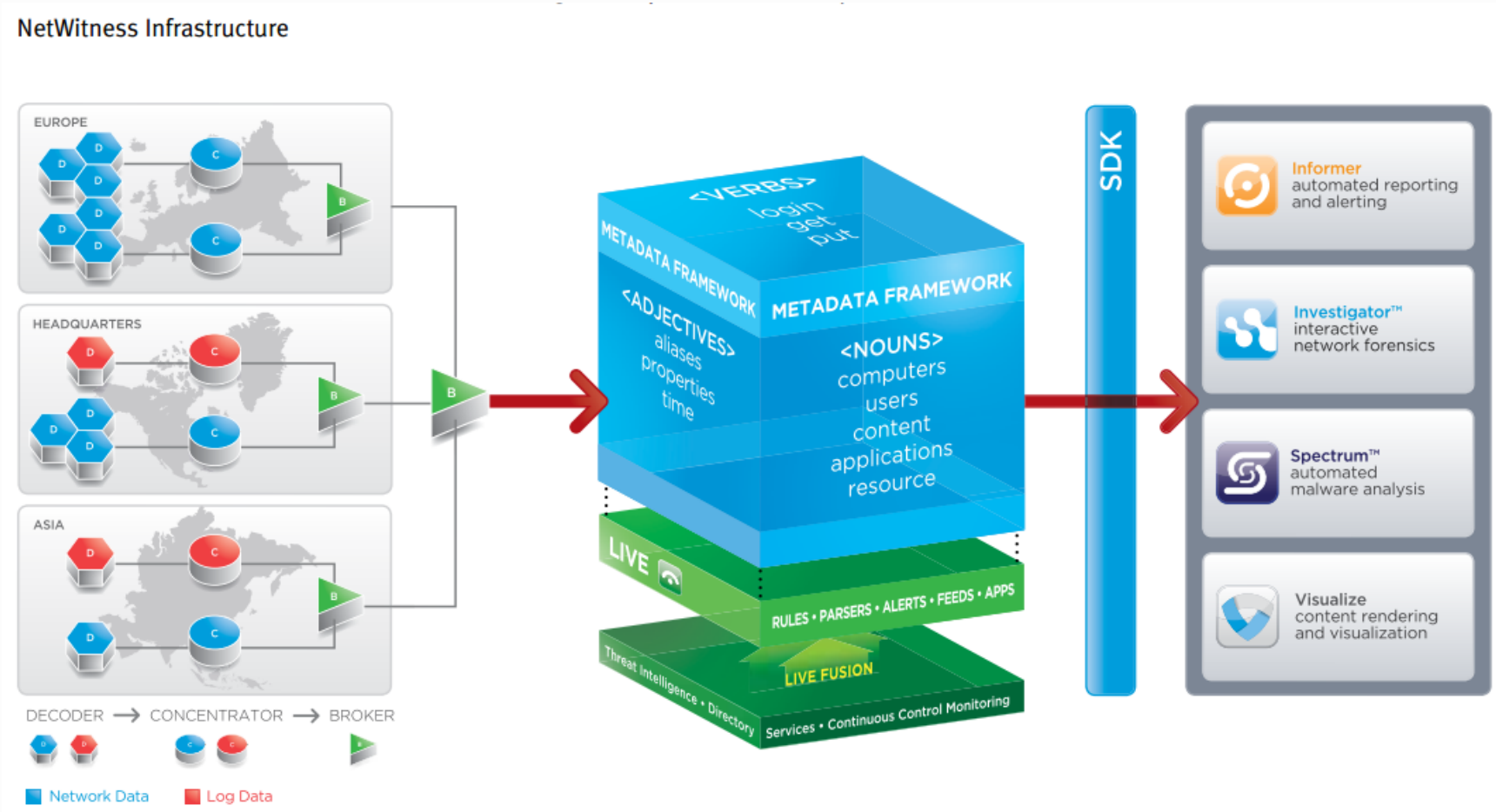
MANDIANT®

《Chinese Advanced Persistent Threats》

日志数据聚合分析和事件重构

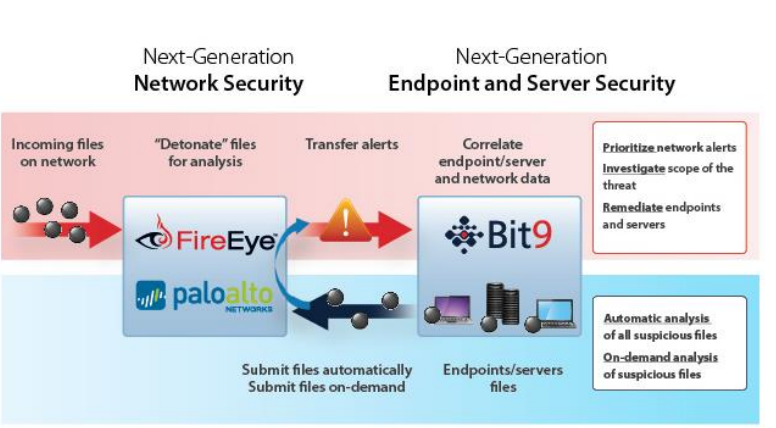
- 采集海量数据：
  - 终端、服务器的各类运行日志和运行数据
  - 网络设备原始流量和事件
  - 外部威胁情报信息
- 集中分析和关联挖掘，发现APT攻击并还原攻击场景和过程
- 典型代表：RSA NetWitness、Solera

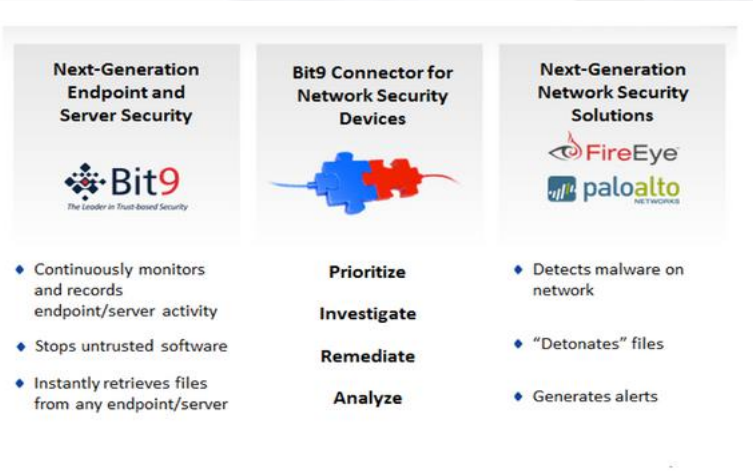
RSA NetWitness



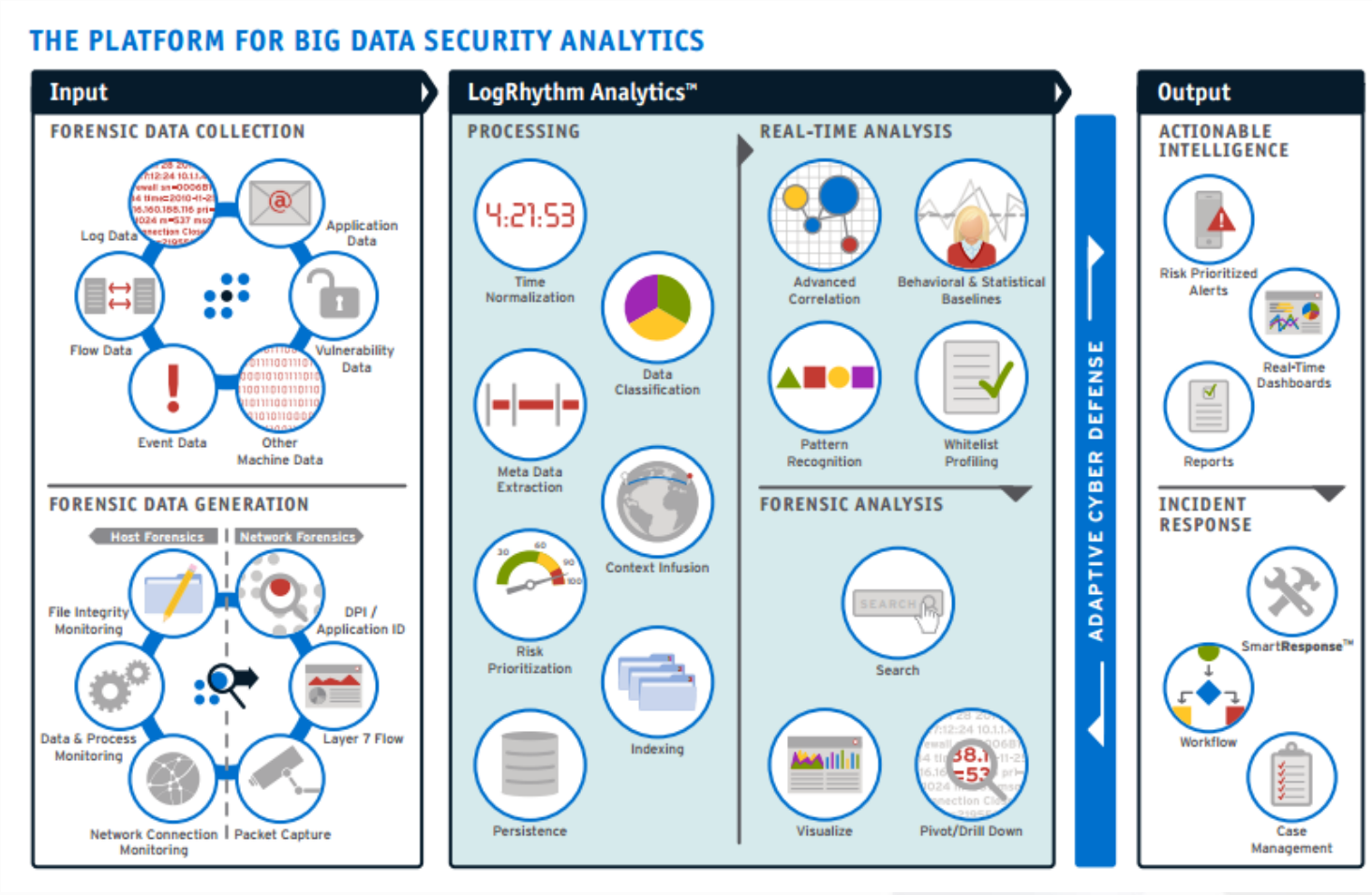
反APT方向的趋势

- 多阶段信息融合，更有效地APT发现
- 实时防御和处置问题
- 多种方案的合作
  - 例如，Bit9与FireEye的集成、FireEye与SIEM的合作

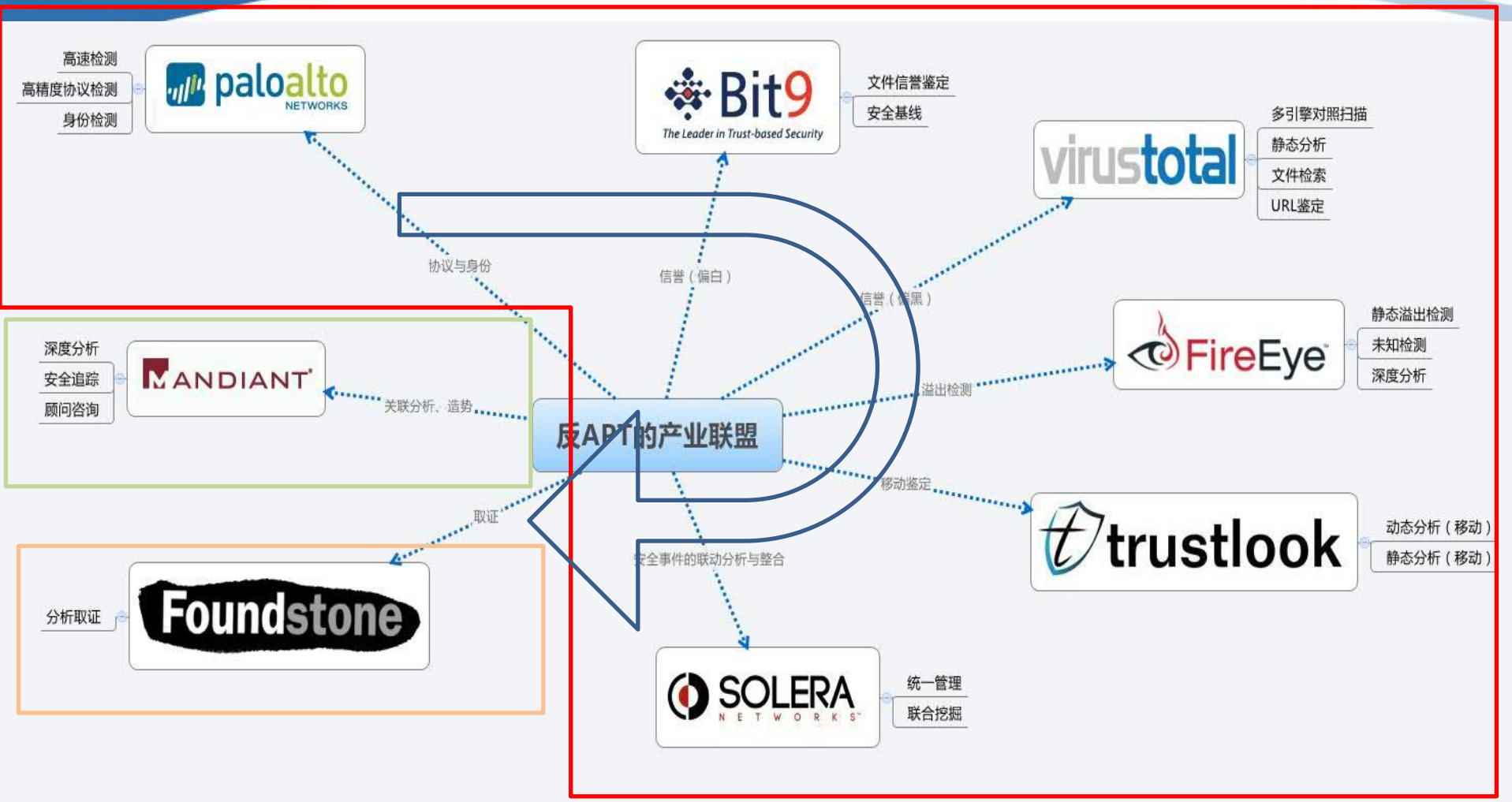




Fire+siem


THE PLATFORM FOR BIG DATA SECURITY ANALYTICS
Input
FORENSIC DATA COLLECTION
Log Data
Application Data
Flow Data
Vulnerability Data
Event Data
Other Machine Data
FORENSIC DATA GENERATION
Host Forensics
Network Forensics
File Integrity Monitoring
DPI / Application ID
Data & Process Monitoring
Layer 7 Flow
Network Connection Monitoring
Packet Capture
LogRhythm Analytics™
PROCESSING
4:21:53
Time Normalization
Data Classification
Meta Data Extraction
Context Infusion
Risk Prioritization
Indexing
Persistence
REAL-TIME ANALYSIS
Advanced Correlation
Behavioral & Statistical Baselines
Pattern Recognition
Whitelist Profiling
FORENSIC ANALYSIS
SEARCH
Search
Visualize
Pivot/Drill Down
ADAPTIVE CYBER DEFENSE
Output
ACTIONABLE INTELLIGENCE
Risk Prioritized Alerts
Real-Time Dashboards
Reports
INCIDENT RESPONSE
SmartResponse™
Workflow
Case Management

反APT的事实产业联盟与作业过程分析



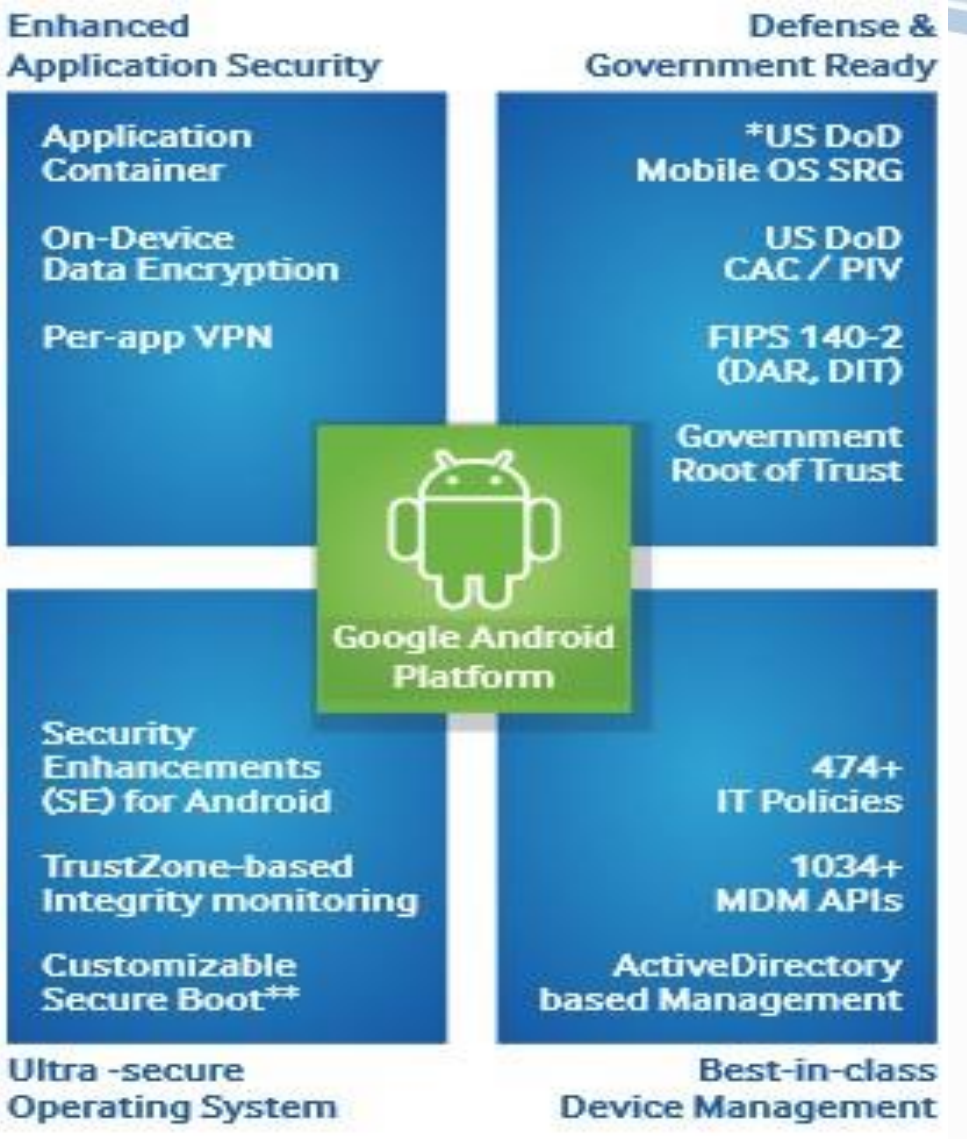
安天实验室制图
2013年9月12日更新

MDM/BYOD

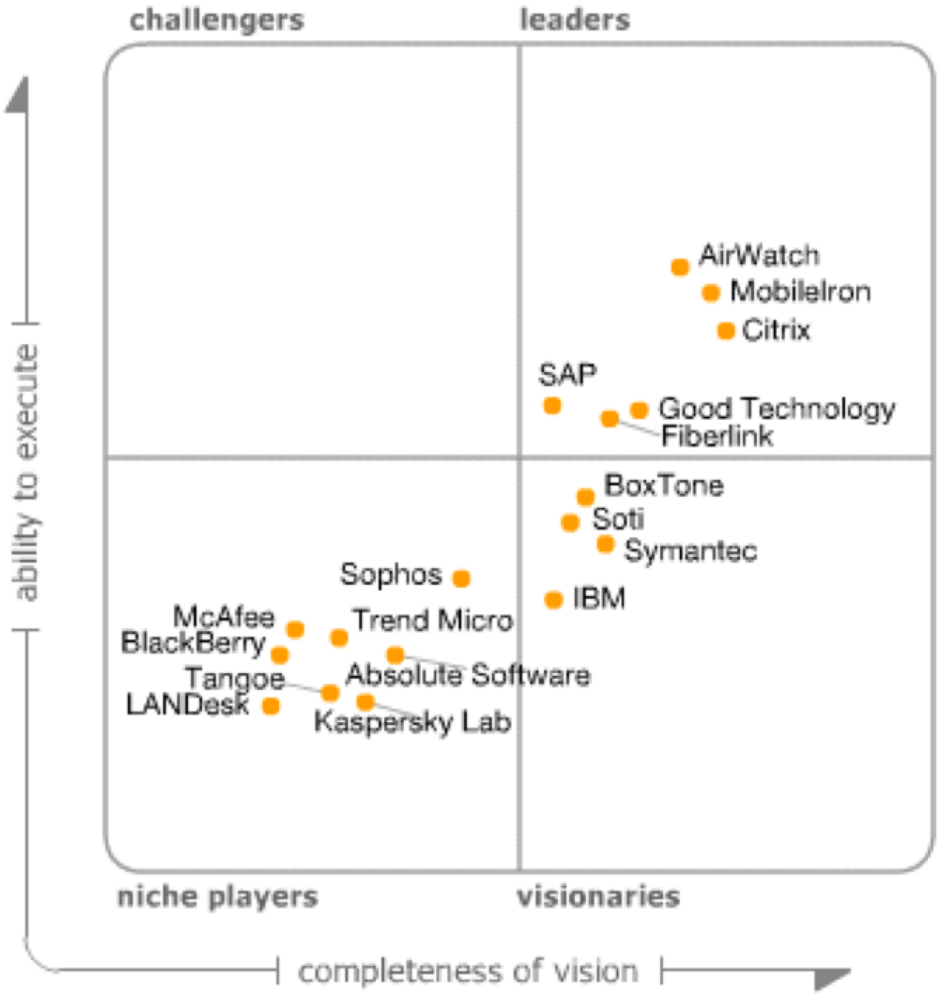
- Mobile Device/Application/Information/Content Management
- Bring Your Own Devices
- 背景：
  - 良好的产业生态和用户习惯下，恶意代码不是西方国家在移动平台的主要威胁
  - 移动设备（包括手机和PC）用于办公环境已成常态，导致安全边界的扩张
  - 定制化办公app的出现和普及

MDM/BYOD的一些内容

- 网络和接入管理
- 数据和资源安全性、服务访问权限
- 应用软件的安全性
- 远程访问安全性
- 人员和策略管理
- 设备安全策略管理（密码、证书、数据清除等）

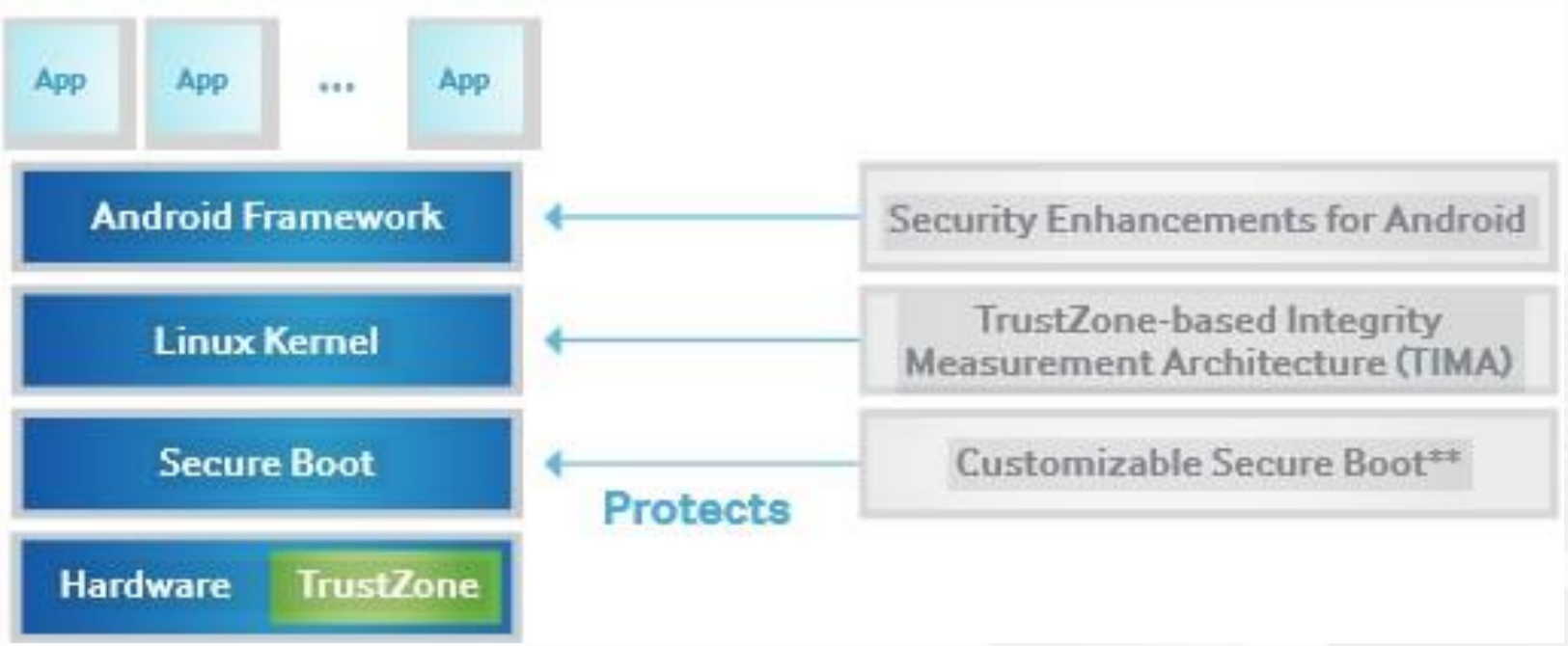


部分现有企业


challengers
leaders
niche players
visionaries
ability to execute
completeness of vision
AirWatch
MobileIron
Citrix
SAP
Good Technology
Fiberlink
BoxTone
Soti
Symantec
IBM
Sophos
McAfee
BlackBerry
Trend Micro
Absolute Software
Tangoe
LANDesk
Kaspersky Lab
Source: Gartner (May 2013)
As of May 2013

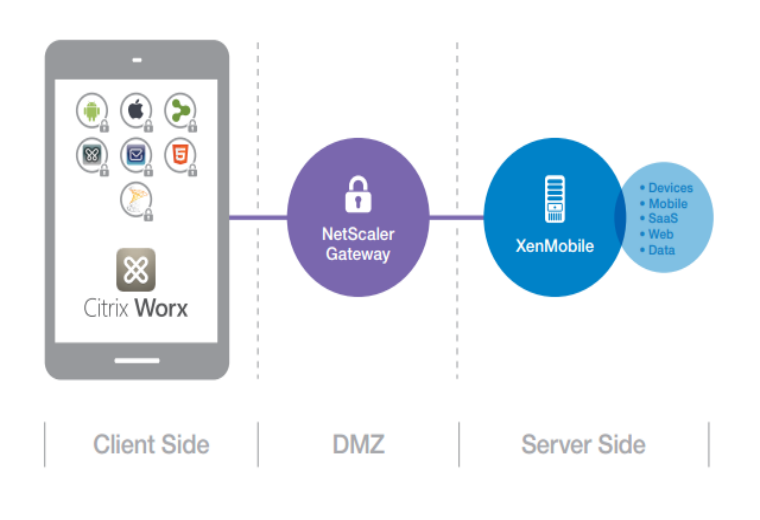
MDM/BYOD方案特色

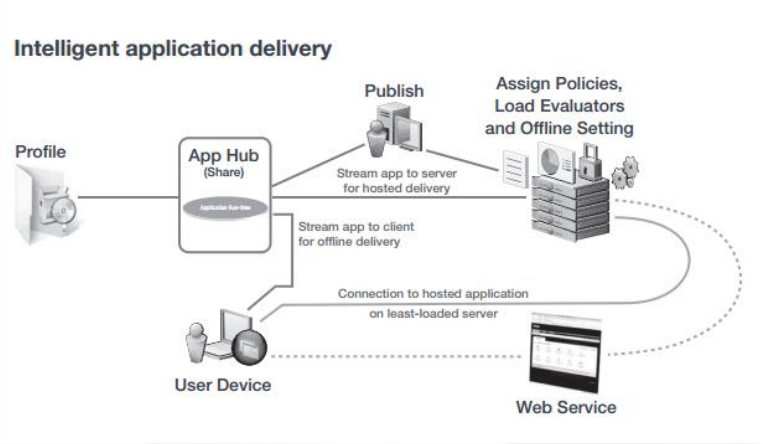
- Samsung Knox：办公和生活场景的应用隔离（系统级支持）、基于SELinux的集中权限控制、内核级加密支持



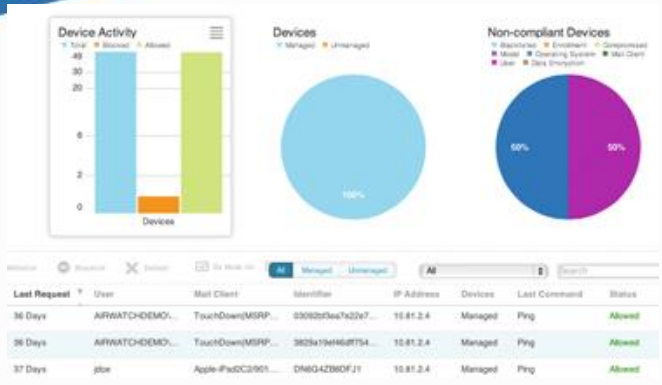
MDM/BYOD方案特色

- Citrix：企业私有商店、现有应用便捷移植、数据私有云存储和便捷访问





airwatch

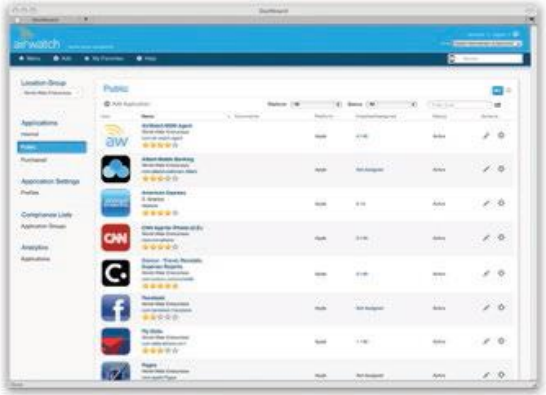


General Email Policies

Active	Policy	Current Compliance Policies
	Managed Device	Allow unmanaged devices
	Mail Client	Allow unlisted clients, Allow Discovered Clients
	User	Allow unlisted users, Allow Discovered Users

Managed Device Policies

Active	Policy	Current Compliance Policies
	Inactivity	Allow Inactive Devices
	Device Compromised	Allow compromised devices



AirWatch：增强移动安全、应用安全管理、基于安全柜的移动内容管理和移动电子邮件管理

MDM/BYOD方案特色

- MobileIron：构建应用级别的沙箱，实现更明确的数据访问保护和网络连接策略

其他

- 云计算和虚拟化安全
- 基于大数据和深度学习的知识发现和态势展现
- 数据安全DLP（Data leakage prevention, DLP）,(Data Loss prevention, DLP)

思考——攻防启示录

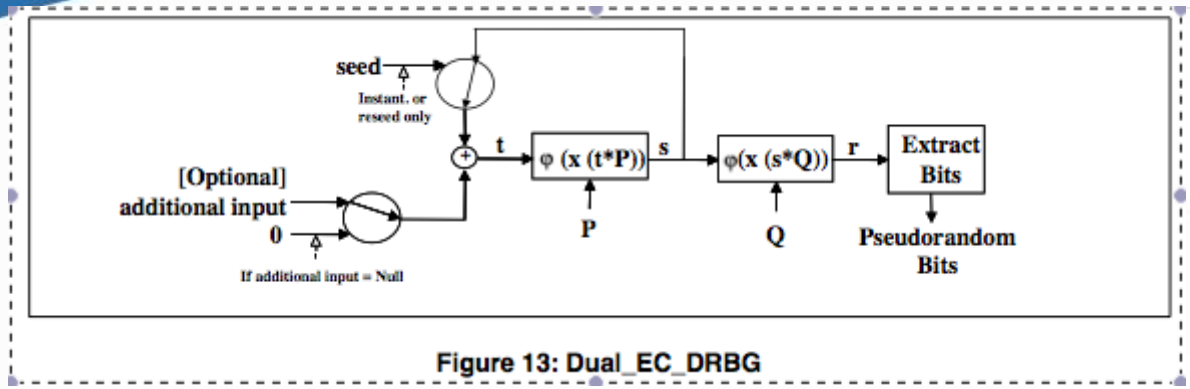
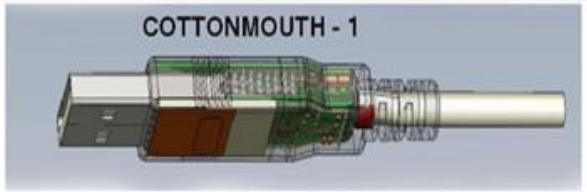
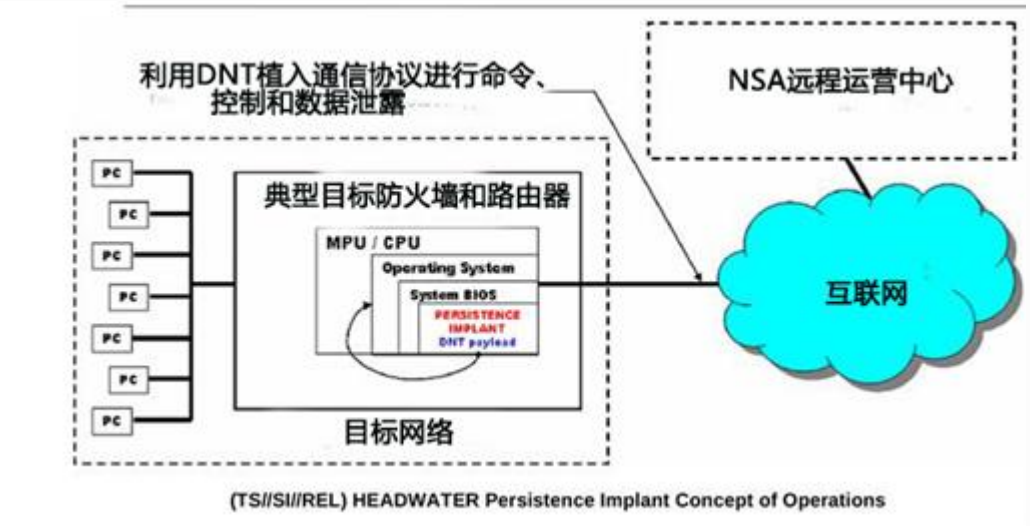
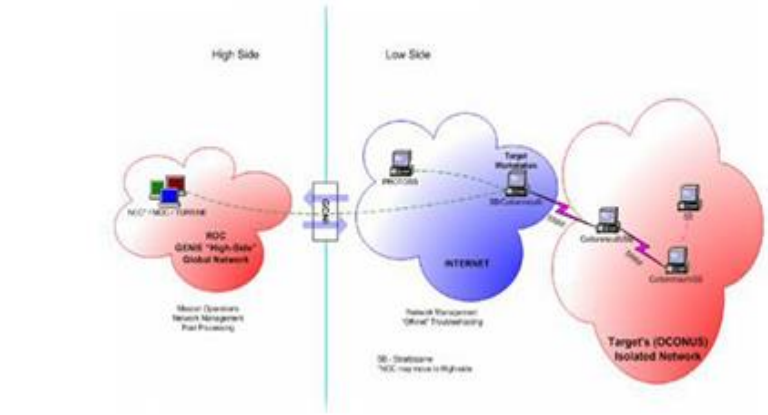


Figure 13: Dual_EC_DRBG





(TS//SI//REL) HEADWATER Persistence Implant Concept of Operations



- 从棱镜门到间谍武器库的攻防启示录。

感谢各位尊敬的专家领导
参加本次研讨会活动

- 肖新光
- seak@antiy.com
- Weibo.com/seak