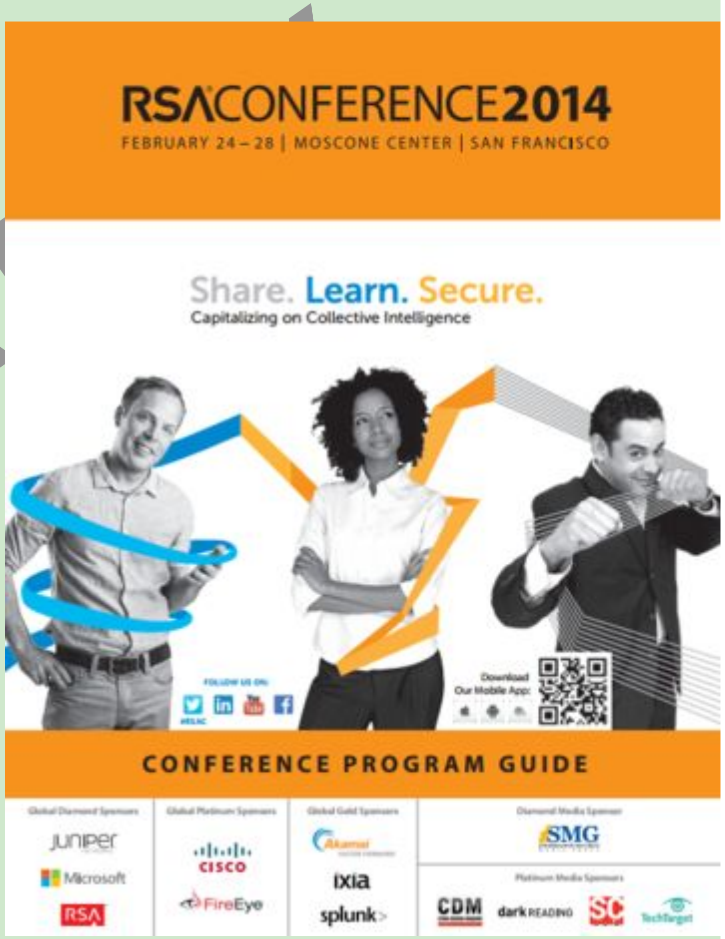
A Glance at RSA Conference 2014
RSA2014 ~ 漫读

赵 粮
Richard Zhao
Chief Strategy Officer, NSFOCUS

April 2014

RSA2014的一些数字

- ❑ 时间
  - 演讲（2/24~2/28），展会（2/25~2/27）
- ❑ 地点
  - 美国旧金山*莫斯科尼*展览中心
- ❑ 大会主题
  - Share•Learn•Secure—*Capitalizing on Collective Intelligence*
  - 分享·学习·加固：*利用集体智慧*
- ❑ 规模
  - *20*多个专题
  - *300*多场演讲
  - *350*多家厂商参展
  - 约*25000*人参加



RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share. Learn. Secure.

Capitalizing on Collective Intelligence

CONFERENCE PROGRAM GUIDE

San Francisco

Moscone Center

有广告...Security Ads at the Streets

有广告...Security Ads at the Streets

Software Defined Protection by Checkpoin

有美女...

RSA
Win Helion Animus
Radio Controlled Truggy
00 value)
VSS
monitoring
Unprecedented TOOL
Visibility and Scale
ENTERPRISE CLOUD
The leader in network intelligence optimization
NMS
Build a Cohesive Optimization Fabric

有猛男...

Homeland Security
Bit9
GHOSTS WANTED
ForeScout
Wicked fast. Deadly accurate.
ForeScout CounterACT™
ForeScout
The Network Security Game Changer.

有名人...

绿盟科技的展台

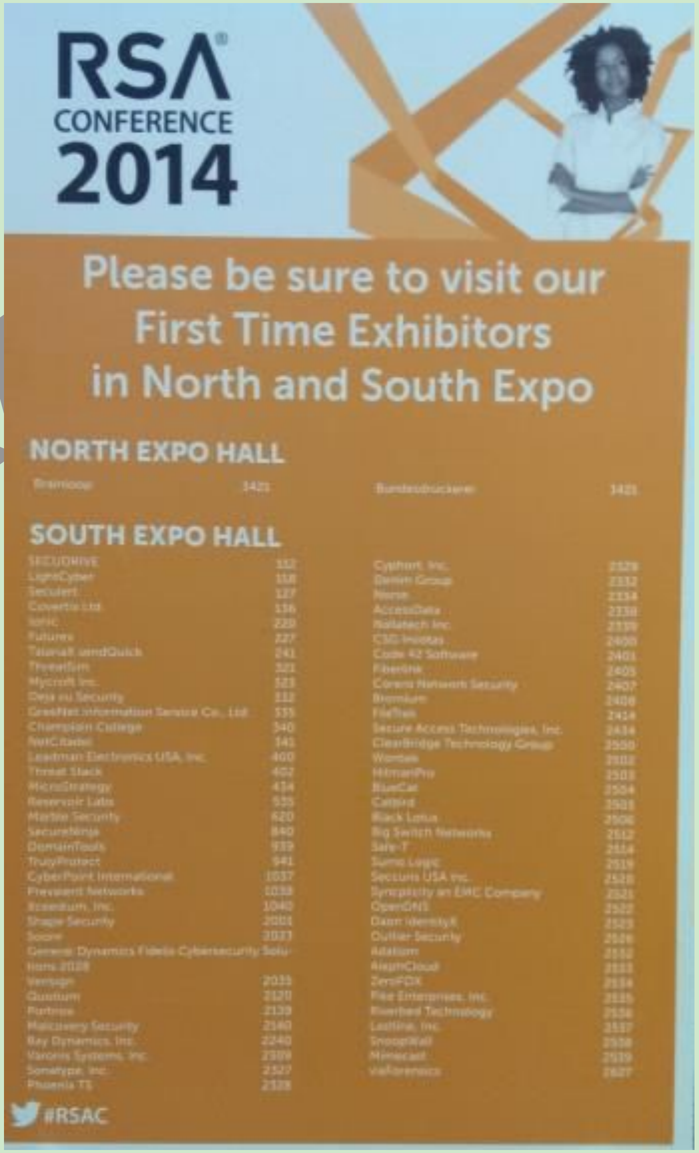
Stop DDoS Attacks
Before They Stop You
WWW.NSFOCUS.COM
defense
WWW.NSFOCUSBLOG.COM
NSFOCUS
Feeling Like
Whac-A-Mole?
WHAC A DDoS ATTACK
DIGITALGUARDIAN
Cyberoam

绿盟科技展台的游戏机 – 砸地鼠

从RSA2014看美国网络安全行业

70 + 新面孔

Black Lotus
Corero Network Security
Catbird
Big Switch
Riverbed
Bromium
Cyphort
Shape Security
Sumologic
…



RSA CONFERENCE 2014

Please be sure to visit our First Time Exhibitors in North and South Expo

NORTH EXPO HALL

Brainloop	3421
Bundesdruckerei	3421

SOUTH EXPO HALL

SECUDRIVE	112
LightCyber	118
Seculert	127
Covertix Ltd	136
Ionic	220
Futurex	227
TalariaX sendQuick	241
ThreatSim	321
Mycroft Inc.	323
Deja vu Security	332
GreatNet Information Service Co., Ltd	335
Champlain College	340
NetCitadel	341
Leadman Electronics USA, Inc.	400
Threat Stack	402
MicroStrategy	434
Reservoir Labs	535
Marble Security	620
SecureNinja	840
DomainTools	939
TrulyProtect	941
CyberPoint International	1037
Prevalent Networks	1038
Ecsendium, Inc.	1040
Shape Security	2001
Socure	2023
General Dynamics Fidelis Cybersecurity Solutions	2028
Verisign	2035
Quantum	2120
Portnox	2139
Malcovery Security	2140
Bay Dynamics, Inc.	2240
Varonis Systems, Inc.	2309
Sonatype, Inc.	2327
Phoenix TS	2328
Cyphort, Inc.	2329
Denim Group	2332
Norse	2334
AccessData	2338
Nallatech Inc.	2339
CSG Invotas	2400
Code 42 Software	2401
Fiberlink	2405
Corero Network Security	2407
Bromium	2408
FileTrek	2414
Secure Access Technologies, Inc.	2434
ClearBridge Technology Group	2500
Wombat	2502
HitmanPro	2503
BlueCat	2504
Catbird	2505
Black Lotus	2506
Big Switch Networks	2512
Safe-T	2514
Sumo Logic	2519
Seccuris USA Inc.	2520
Syncplicity an EMC Company	2521
OpenDNS	2522
Daon IdentityX	2523
Outlier Security	2526
Adallom	2532
AlephCloud	2533
ZeroFOX	2534
Fike Enterprises, Inc.	2535
Riverbed Technology	2536
Lastline, Inc.	2537
SnoopWall	2538
Mimecast	2539
viaForensics	2627

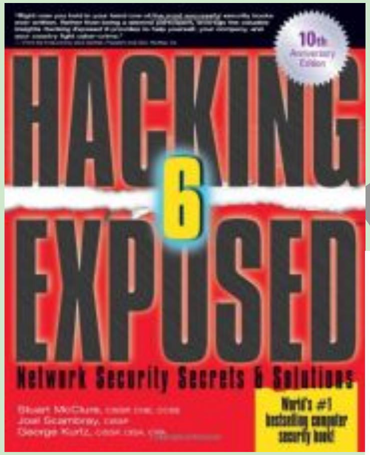
#RSAC

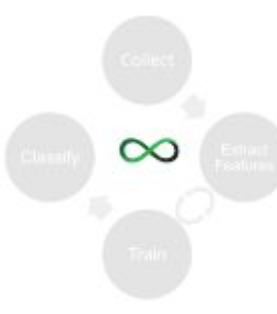
RSA每年的创新沙盒吸引众多目光

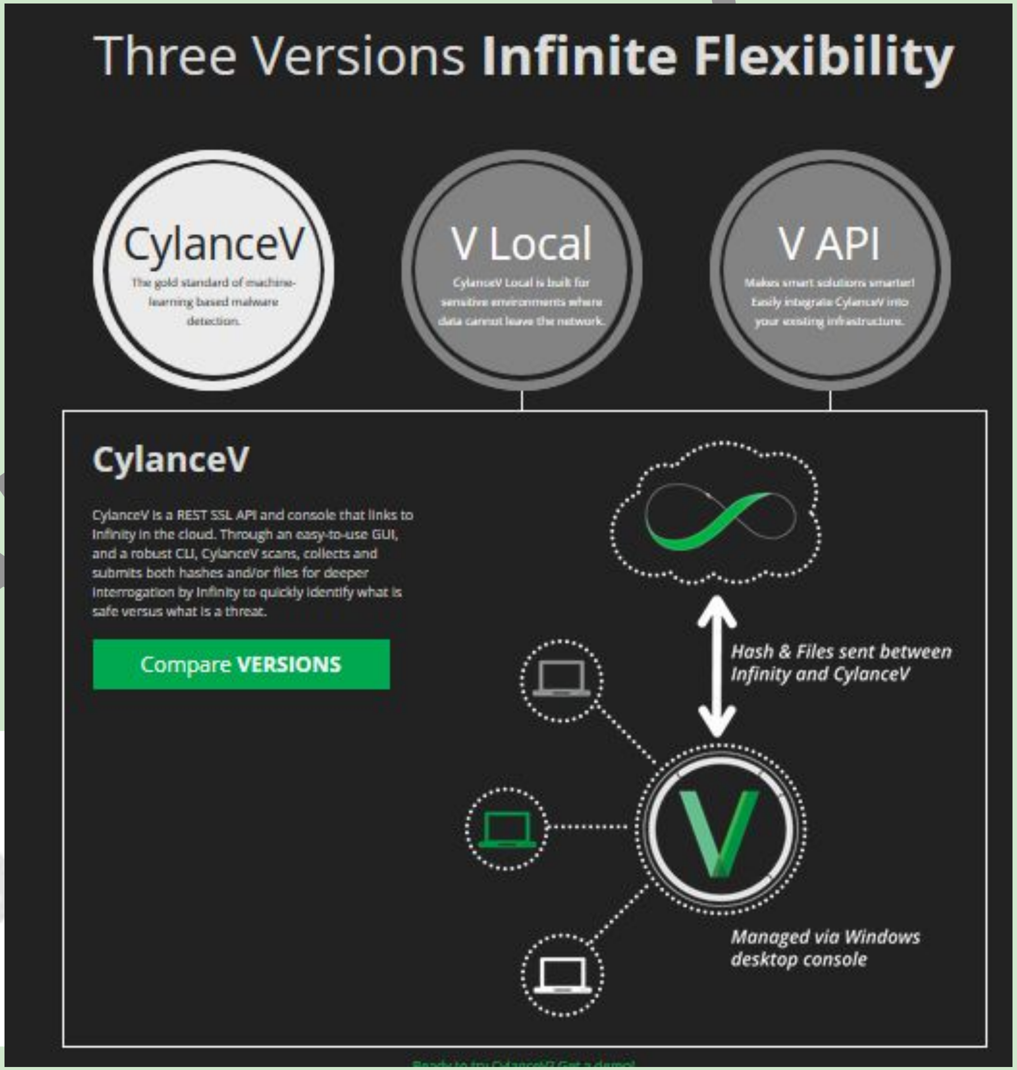
2014 10 Finalists, half of them are APT with data analytics.

RedOwl荣获创新沙盒冠军

CYLANCE


10th Anniversary Edition
HACKING EXPOSED 6
Network Security Secrets & Solutions
Stuart McClure
Joel Scambray
George Kurtz
World's #1 bestselling computer security book!





Three Versions **Infinite Flexibility**

CylanceV
The gold standard of machine-learning based malware detection.

V Local
CylanceV Local is built for sensitive environments where data cannot leave the network.

V API
Makes smart solutions smarter! Easily integrate CylanceV into your existing infrastructure.

CylanceV

CylanceV is a REST SSL API and console that links to Infinity in the cloud. Through an easy-to-use GUI, and a robust CLI, CylanceV scans, collects and submits both hashes and/or files for deeper interrogation by Infinity to quickly identify what is safe versus what is a threat.

Compare **VERSIONS**

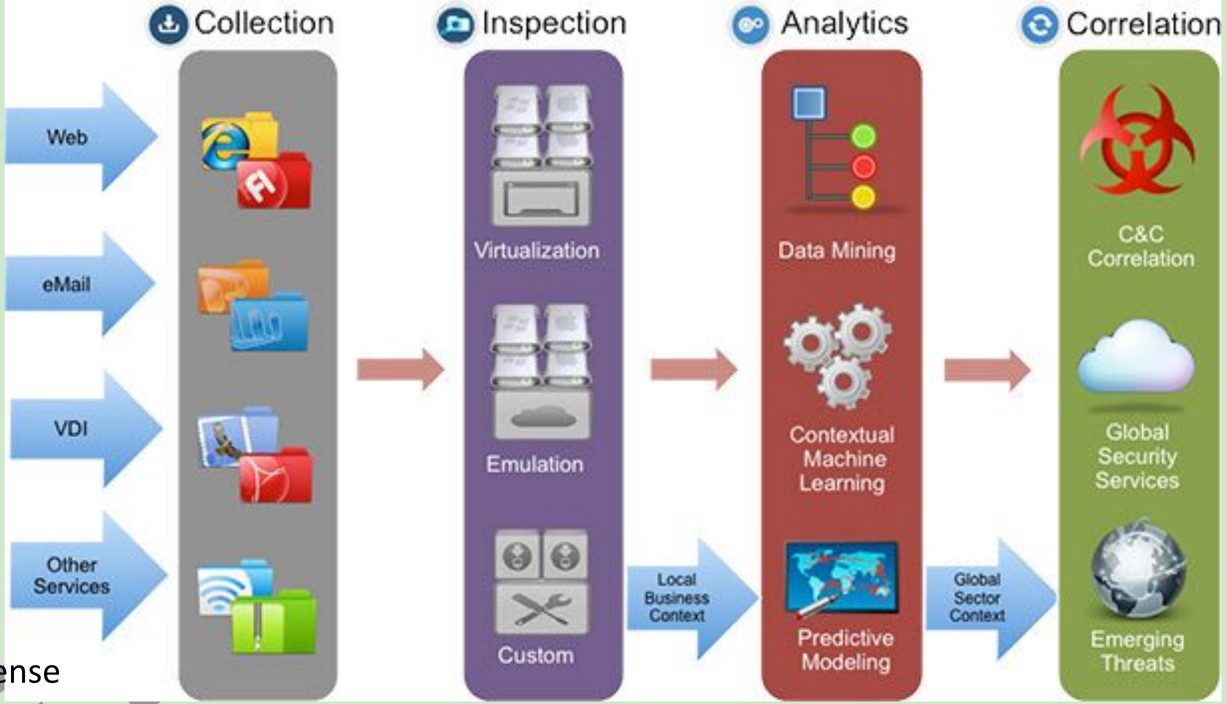
Hash & Files sent between Infinity and CylanceV
Managed via Windows desktop console

Ready to try CylanceV? Get a demo!

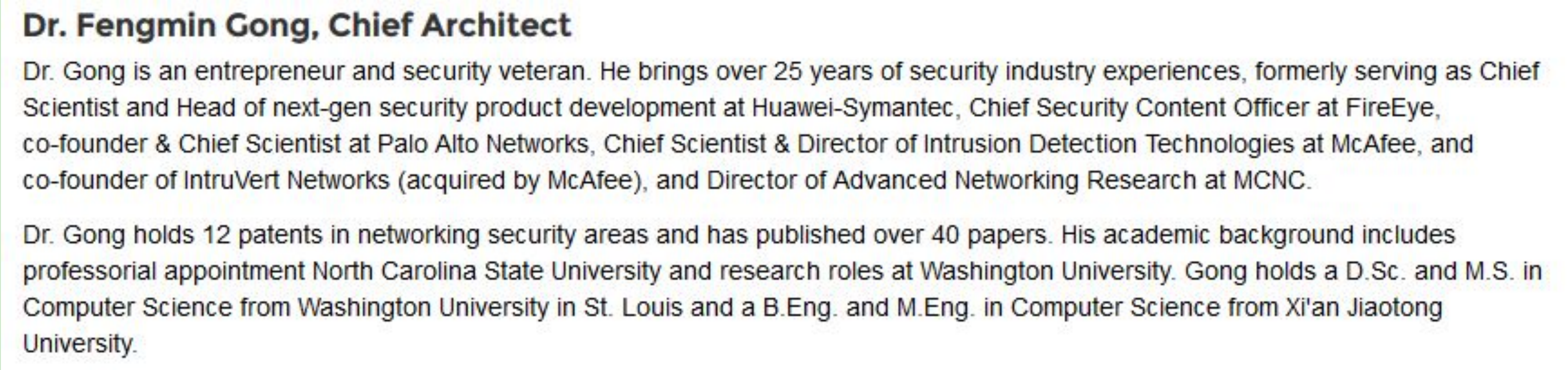
http://cylance.com/products.shtml#cylance-protect

CYPHORT , a Startup

CYPHORT



ATD: Advanced Threat Defense



Dr. Fengmin Gong, Chief Architect

Dr. Gong is an entrepreneur and security veteran. He brings over 25 years of security industry experiences, formerly serving as Chief Scientist and Head of next-gen security product development at Huawei-Symantec, Chief Security Content Officer at FireEye, co-founder & Chief Scientist at Palo Alto Networks, Chief Scientist & Director of Intrusion Detection Technologies at McAfee, and co-founder of IntruVert Networks (acquired by McAfee), and Director of Advanced Networking Research at MCNC.

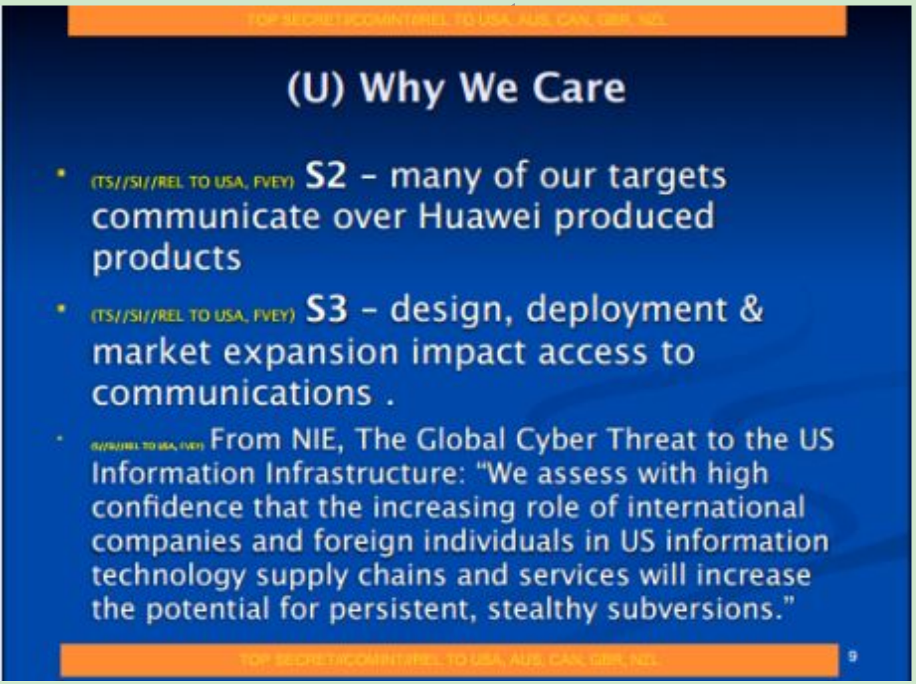
Dr. Gong holds 12 patents in networking security areas and has published over 40 papers. His academic background includes professorial appointment North Carolina State University and research roles at Washington University. Gong holds a D.Sc. and M.S. in Computer Science from Washington University in St. Louis and a B.Eng. and M.Eng. in Computer Science from Xi'an Jiaotong University.

RSA2014之前发生的事情

@2013，FireEye上市 – Mandiant发布APT1报告 – FireEye收购Mand

Mr.Snowden, PRISM, Shotgiant…

The whistleblower
I can't allow the US government to destroy privacy and basic liberties
theguardian
guardian.co.uk



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) Why We Care

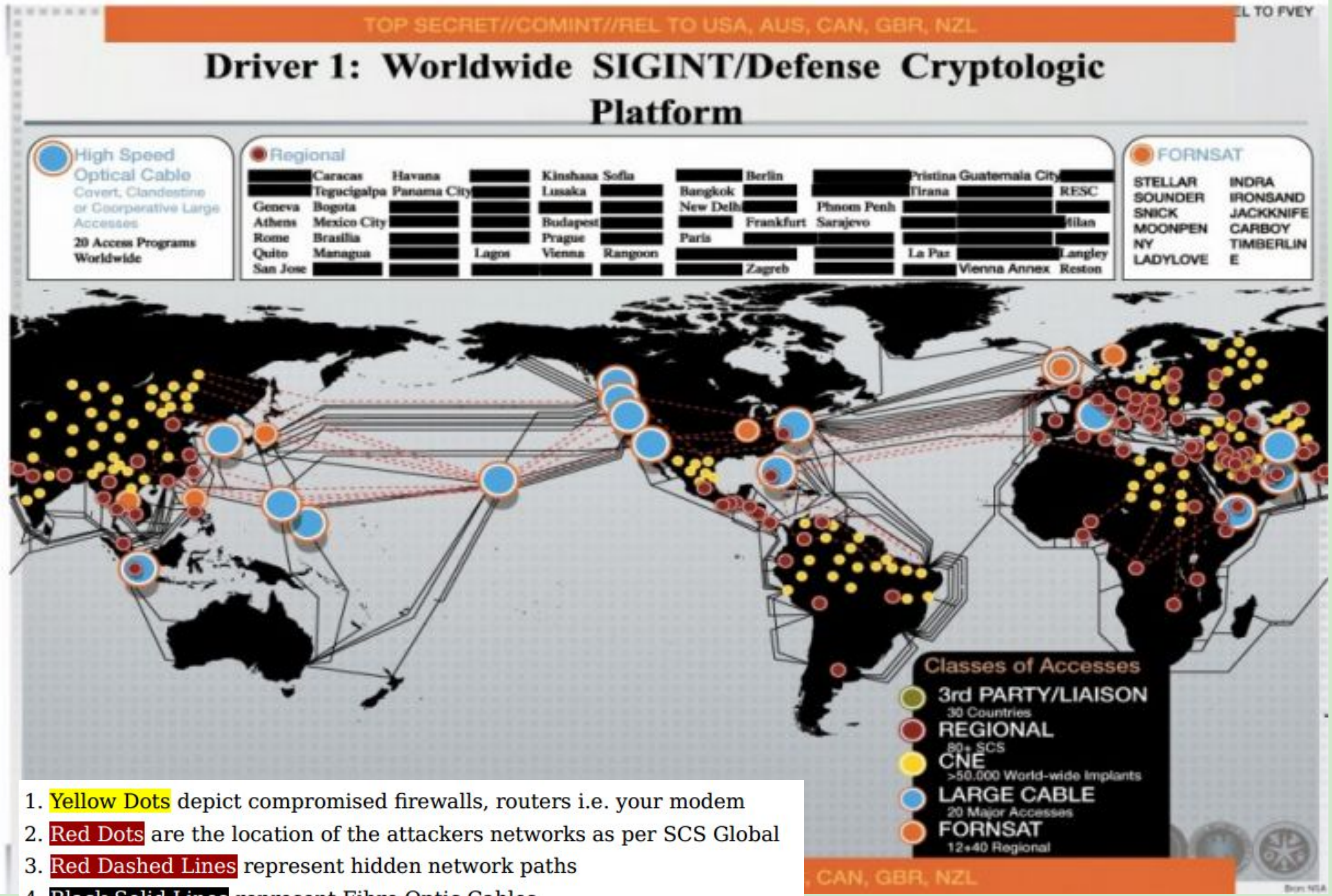
- (TS//SI//REL TO USA, FVEY) **S2** – many of our targets communicate over Huawei produced products
- (TS//SI//REL TO USA, FVEY) **S3** – design, deployment & market expansion impact access to communications .
- (S//SI//REL TO USA, FVEY) From NIE, The Global Cyber Threat to the US Information Infrastructure: "We assess with high confidence that the increasing role of international companies and foreign individuals in US information technology supply chains and services will increase the potential for persistent, stealthy subversions."

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

9

"The irony is that exactly what they are doing to us is what they have always charged that the Chinese are doing through us." *- William Plummer, a senior Huawei executive in the United States*

Cyber Warfare and Intelligence



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

EL TO FVEY

Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

High Speed Optical Cable

Covert, Clandestine or Coorperative Large Accesses

20 Access Programs Worldwide

Regional

[redacted]	Caracas	Havana	[redacted]	Kinshasa	Sofia	[redacted]	Berlin	[redacted]	Pristina	Guatemala City	[redacted]
[redacted]	Tegucigalpa	Panama City	[redacted]	Lusaka	[redacted]	Bangkok	[redacted]	[redacted]	Tirana	[redacted]	RESC
Geneva	Bogota	[redacted]	[redacted]	[redacted]	[redacted]	New Delh	[redacted]	Phnom Penh	[redacted]	[redacted]	[redacted]
Athens	Mexico City	[redacted]	[redacted]	Budapest	[redacted]	[redacted]	Frankfurt	Sarajevo	[redacted]	[redacted]	ilan
Rome	Brasilia	[redacted]	[redacted]	Prague	[redacted]	Paris	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Quito	Managua	[redacted]	Lagos	Vienna	Rangoon	[redacted]	[redacted]	[redacted]	La Paz	[redacted]	Langley
San Jose	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Zagreb	[redacted]	[redacted]	Vienna Annex	Reston

FORNSAT

STELLAR	INDRA
SOUNDER	IRONSAND
SNICK	JACKKNIFE
MOONPEN	CARBOY
NY	TIMBERLIN E
LADYLOVE	

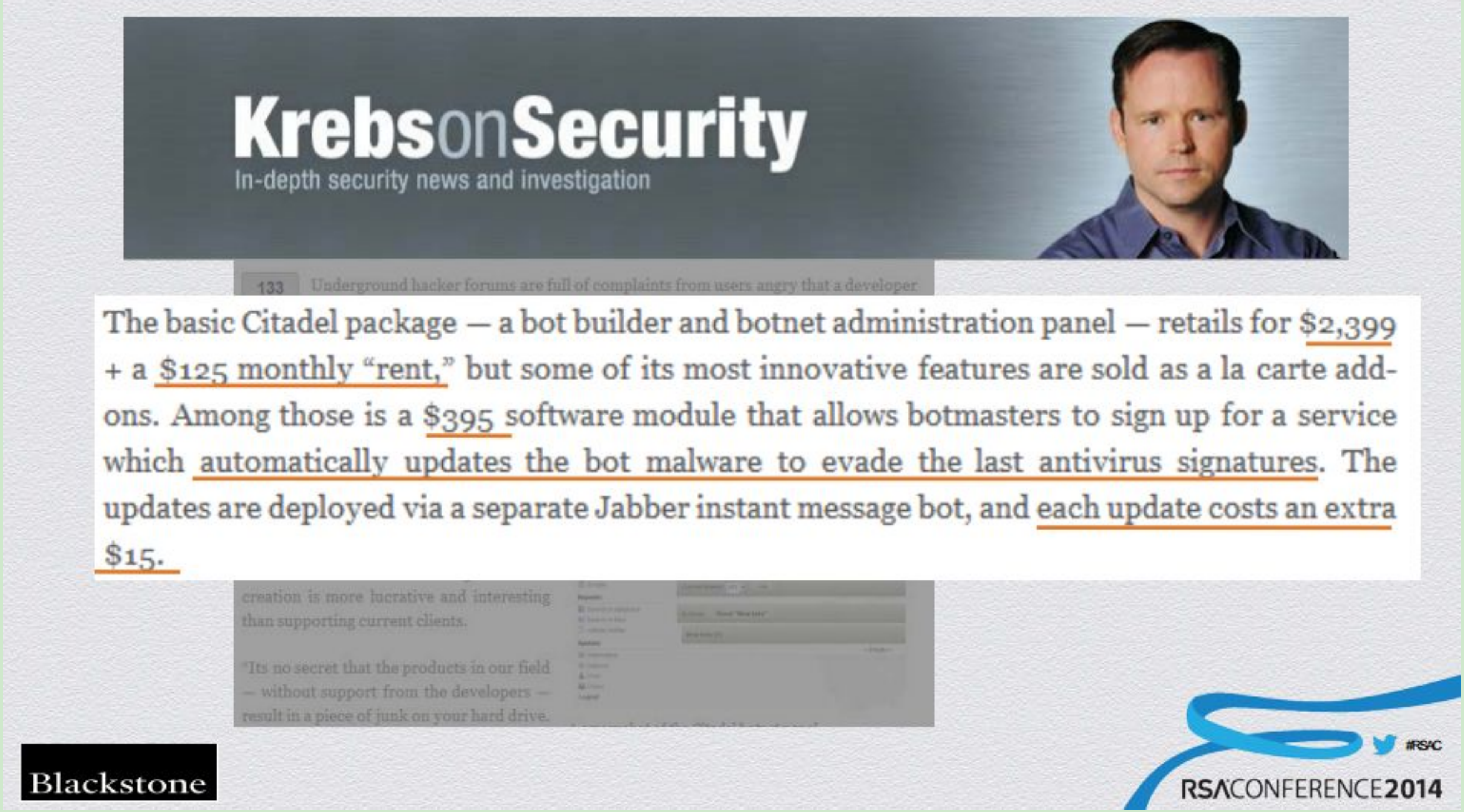
Classes of Accesses

- 3rd PARTY/LIAISON 30 Countries
- REGIONAL 80+ SCS
- CNE >50.000 World-wide Implants
- LARGE CABLE 20 Major Accesses
- FORNSAT 12+40 Regional

, CAN, GBR, NZL

1. Yellow Dots depict compromised firewalls, routers i.e. your modem
2. Red Dots are the location of the attackers networks as per SCS Global
3. Red Dashed Lines represent hidden network paths
4. Black Solid Lines represent Fibre Optic Cables

APT as a Service吗？



133 Underground hacker forums are full of complaints from users angry that a developer

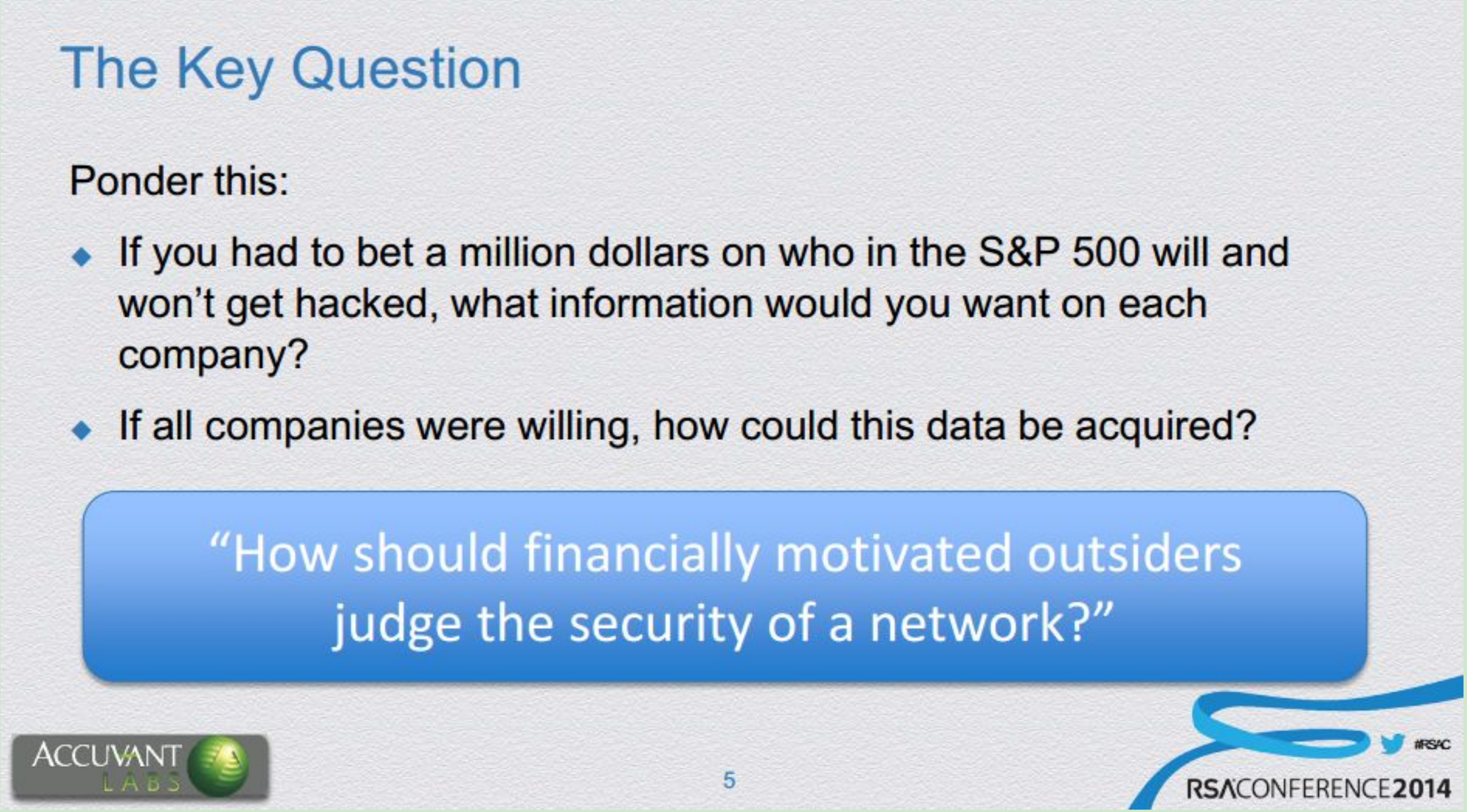
The basic Citadel package — a bot builder and botnet administration panel — retails for $2,399 + a $125 monthly "rent," but some of its most innovative features are sold as a la carte add-ons. Among those is a $395 software module that allows botmasters to sign up for a service which automatically updates the bot malware to evade the last antivirus signatures. The updates are deployed via a separate Jabber instant message bot, and each update costs an extra $15.

creation is more lucrative and interesting than supporting current clients.

"Its no secret that the products in our field — without support from the developers — result in a piece of junk on your hard drive.

RSA2014: str-f02-a-cisos-perspective-v2

这个问题问得深刻



The Key Question

Ponder this:

- If you had to bet a million dollars on who in the S&P 500 will and won’t get hacked, what information would you want on each company?
- If all companies were willing, how could this data be acquired?

> “How should financially motivated outsiders judge the security of a network?”

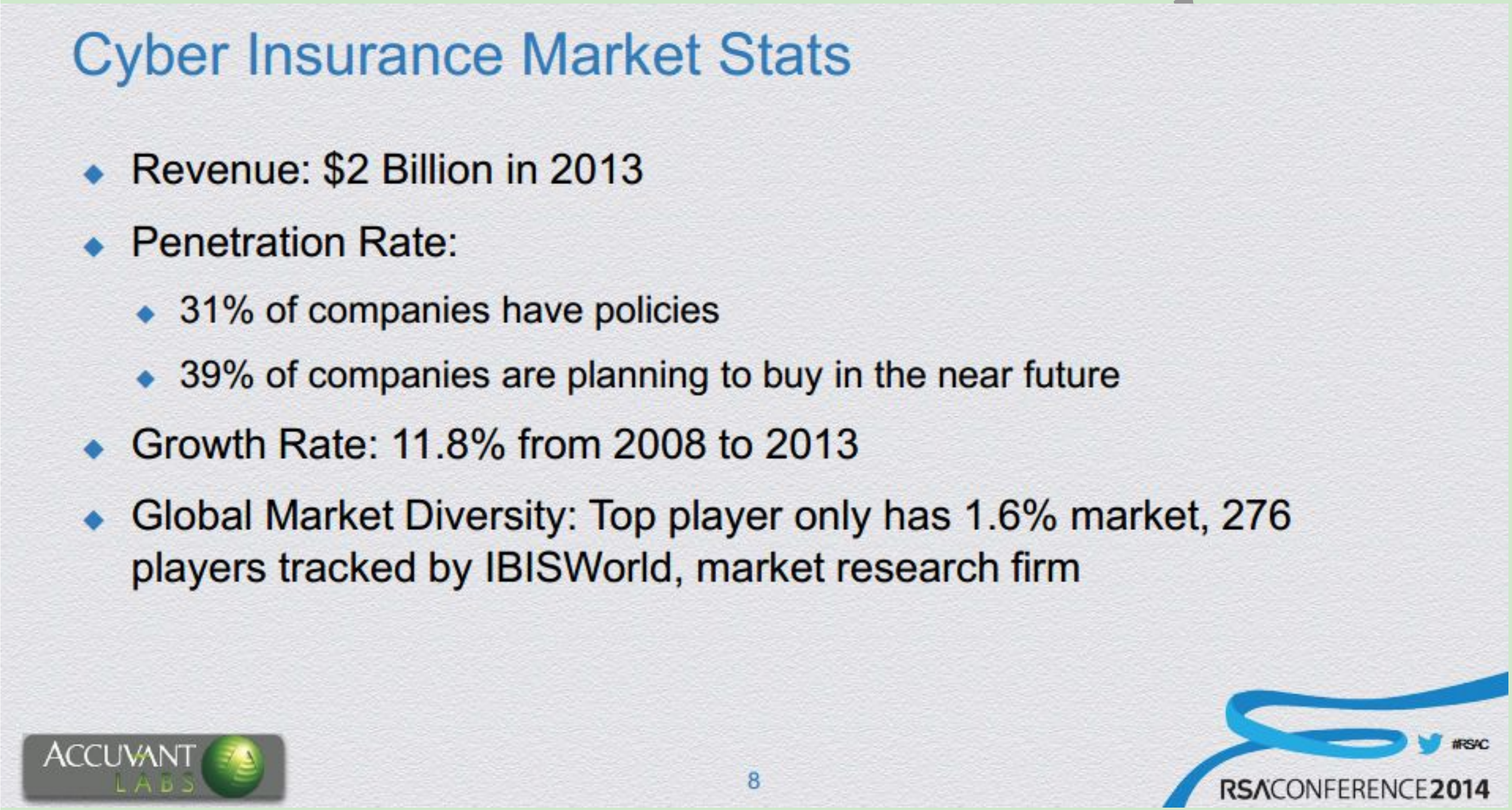
ACCUVANT LABS

#RSAC

RSACONFERENCE2014

RSA2014：grc-w01-adventures-in-insurance-land-weaknesses-in-risk-pricing-and-alternatives

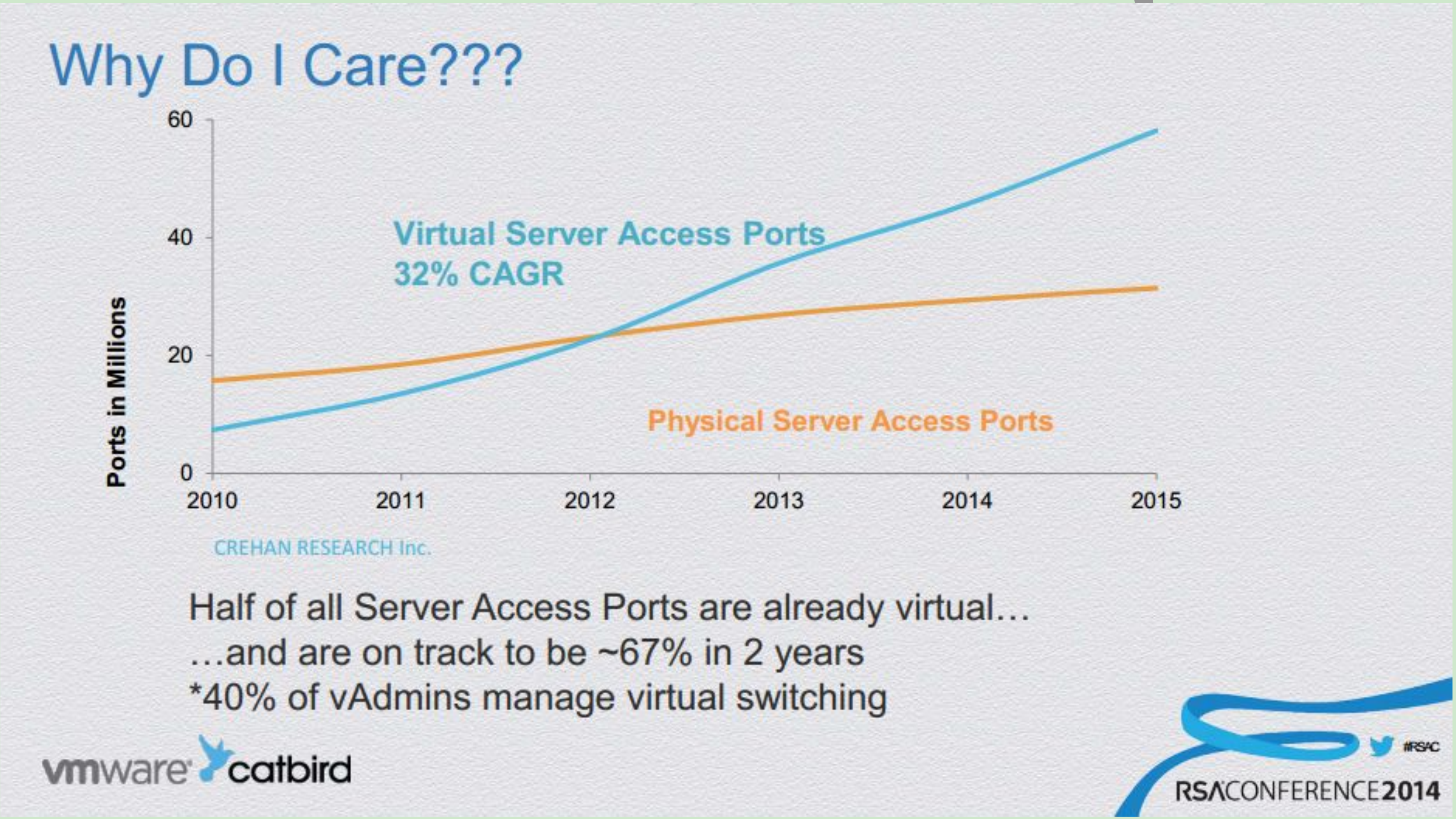
值得我们关注和思索的一些数字



Cyber Insurance Market Stats

- Revenue: $2 Billion in 2013
- Penetration Rate:
  - 31% of companies have policies
  - 39% of companies are planning to buy in the near future
- Growth Rate: 11.8% from 2008 to 2013
- Global Market Diversity: Top player only has 1.6% market, 276 players tracked by IBISWorld, market research firm

虚拟化/云计算/软件定义数据中心

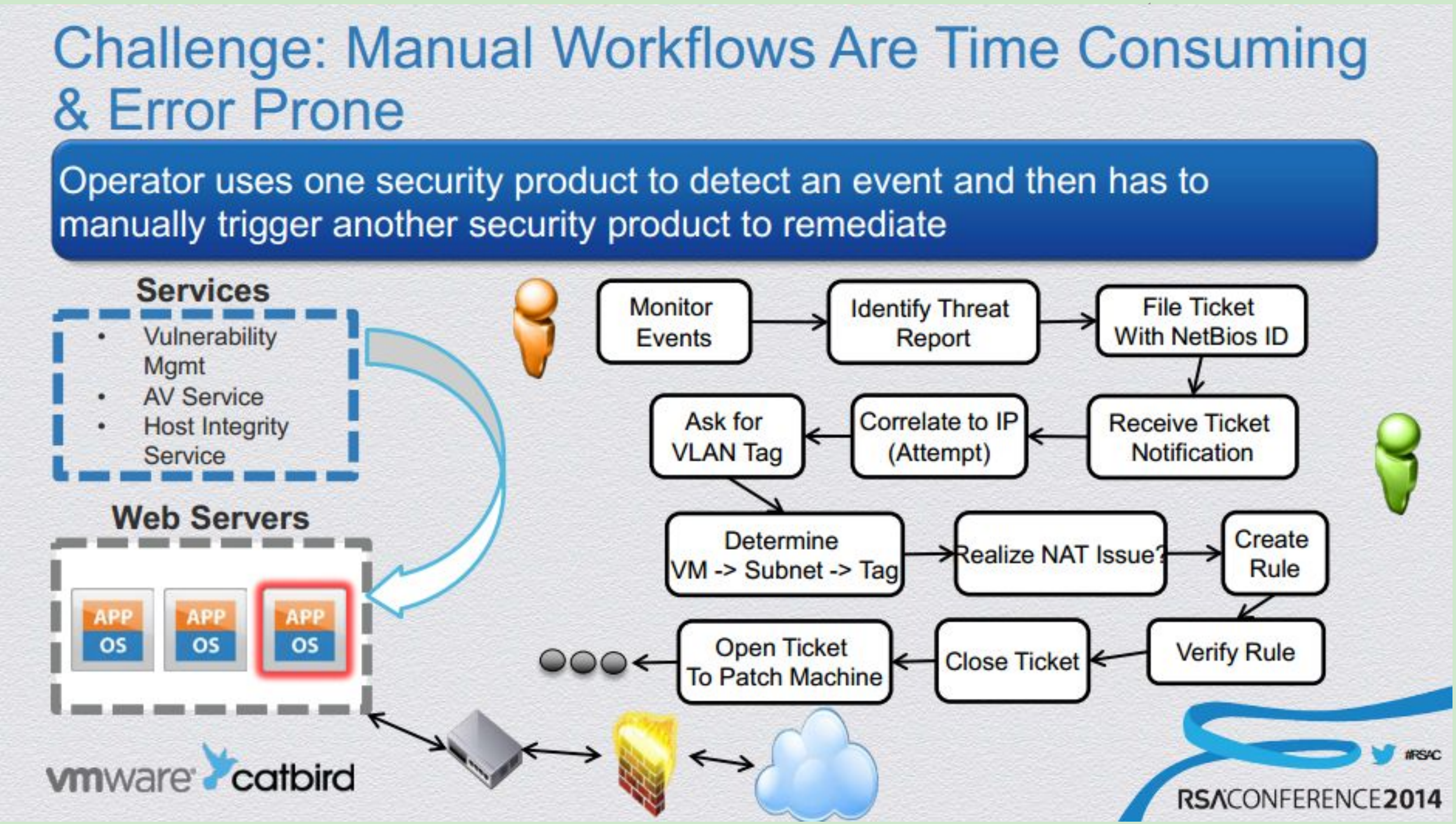


Why Do I Care???

CREHAN RESEARCH Inc.

Half of all Server Access Ports are already virtual…
…and are on track to be ~67% in 2 years
*40% of vAdmins manage virtual switching

SDDC带来的挑战



Challenge: Manual Workflows Are Time Consuming & Error Prone

Operator uses one security product to detect an event and then has to manually trigger another security product to remediate

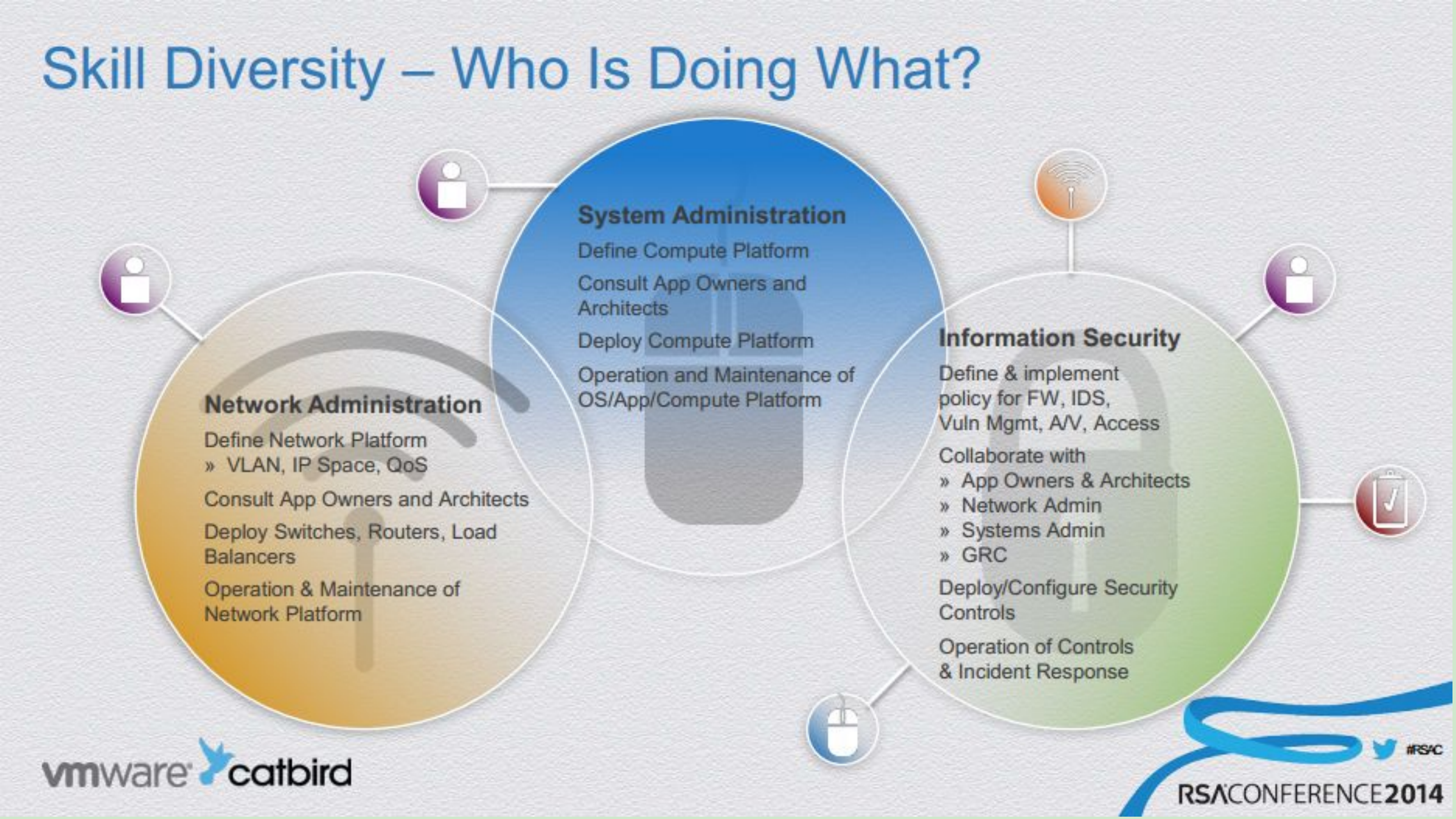
Services

- Vulnerability Mgmt
- AV Service
- Host Integrity Service

Web Servers

Monitor Events → Identify Threat Report → File Ticket With NetBios ID → Receive Ticket Notification → Correlate to IP (Attempt) → Ask for VLAN Tag → Determine VM -> Subnet -> Tag → Realize NAT Issue? → Create Rule → Verify Rule → Close Ticket → Open Ticket To Patch Machine

对职业发展规划带来的启示



Skill Diversity – Who Is Doing What?

System Administration

Define Compute Platform

Consult App Owners and Architects

Deploy Compute Platform

Operation and Maintenance of OS/App/Compute Platform

Network Administration

Define Network Platform
» VLAN, IP Space, QoS

Consult App Owners and Architects

Deploy Switches, Routers, Load Balancers

Operation & Maintenance of Network Platform

Information Security

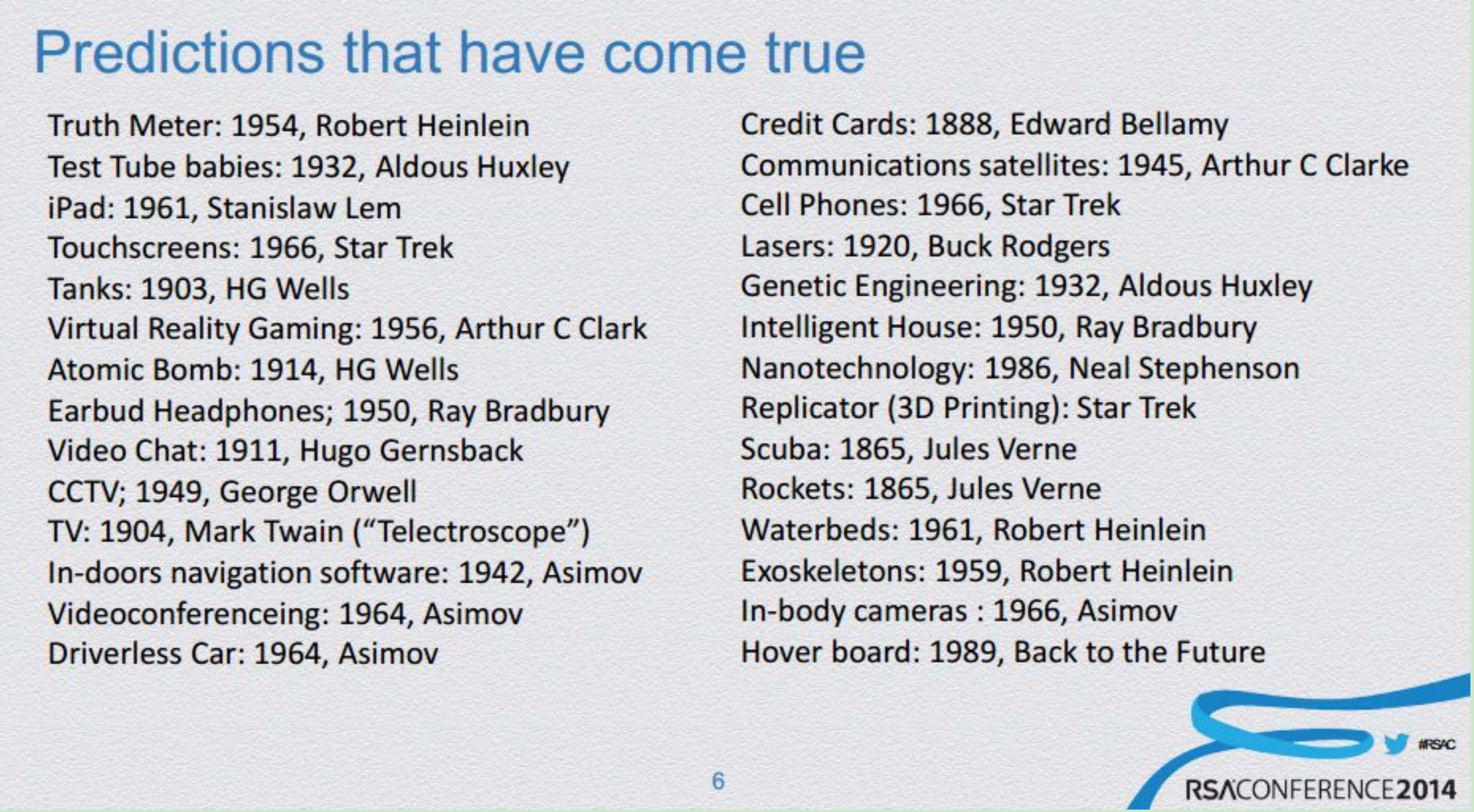
Define & implement policy for FW, IDS, Vuln Mgmt, A/V, Access

Collaborate with
» App Owners & Architects
» Network Admin
» Systems Admin
» GRC

Deploy/Configure Security Controls

Operation of Controls & Incident Response

是否还记得昨天的科幻



Predictions that have come true

Truth Meter: 1954, Robert Heinlein
Test Tube babies: 1932, Aldous Huxley
iPad: 1961, Stanislaw Lem
Touchscreens: 1966, Star Trek
Tanks: 1903, HG Wells
Virtual Reality Gaming: 1956, Arthur C Clark
Atomic Bomb: 1914, HG Wells
Earbud Headphones; 1950, Ray Bradbury
Video Chat: 1911, Hugo Gernsback
CCTV; 1949, George Orwell
TV: 1904, Mark Twain (“Telectroscope”)
In-doors navigation software: 1942, Asimov
Videoconferenceing: 1964, Asimov
Driverless Car: 1964, Asimov

Credit Cards: 1888, Edward Bellamy
Communications satellites: 1945, Arthur C Clarke
Cell Phones: 1966, Star Trek
Lasers: 1920, Buck Rodgers
Genetic Engineering: 1932, Aldous Huxley
Intelligent House: 1950, Ray Bradbury
Nanotechnology: 1986, Neal Stephenson
Replicator (3D Printing): Star Trek
Scuba: 1865, Jules Verne
Rockets: 1865, Jules Verne
Waterbeds: 1961, Robert Heinlein
Exoskeletons: 1959, Robert Heinlein
In-body cameras : 1966, Asimov
Hover board: 1989, Back to the Future

RSA2014: stu-m04a-science-fiction-is-here

思考…

Share. Learn. Secure.

Capitalizing on Collective Intelligence

SECURITY REDEFINED

INTELLIGENCE-DRIVEN SECURITY

Thanks

安全+ 2014/04 总第024

SECURITY

技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

面向安全的大数据分析方法和思路

商业银行信息科技风险管理状况行业对比分析

php.net被植入恶意代码分析

工业控制系统的安全研究与实践

扫一扫 关注绿盟科技官方微信

新浪微博：
@赵粮
@绿盟科技

可以在www.nsfocus.com下载电子版
http://www.nsfocus.com/6_about/6_9.html