

创新与安全技术趋势

Innovation & Security Technology Trends - Silicon Valley Perspective



Dr. Fengmin Gong
Co-Founder & Chief Architect

Topics Of Conversation

- Sustained Competitiveness Requires Sustained Innovation
- Building Best Tools Require Understanding Of <problem, users, environments>
- Security Threat & Technology Trends
- Security Technology Innovation Framework
- Cyphort Product Example

硅谷之成功人人皆知 Silicon Valley Successes

- Total of 18 investment regions in US tracked by MoneyTree Report
- Silicon Valley accounts more than 54% of the total: \$7.09b/\$12.96b (Q2-2014)

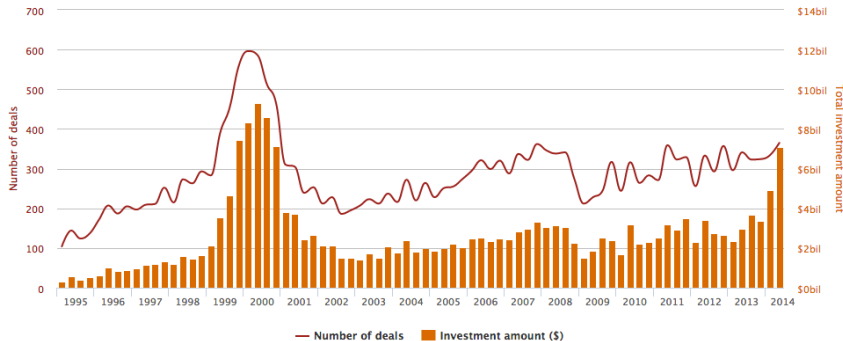
Historical trend data

The chart below shows the aggregated investment dollars and the number of deals from Q1 1995 to Q2 2014.

[Download](#)

Historical trend data

Source: PwC/NVCA MoneyTree™ Report, Data: Thomson Reuters



创业竞争激烈 Survive The Fittest

- 先烈榜样不胜枚举 - for every success there are at least 9 died of quiet death
 - CB Insights, updated June 3, 2014, “76 Startup Failure Post Mortems”, www.cbinsights.com/blog/startup-failure-post-mortem/
 - CB Insights, June 14, “76 of the Biggest, Costliest Startup Failures of All Time”, www.cbinsights.com/blog/biggest-startup-failures/

Title: A startup postmortem with a happy ending? ...in Thailand

Company: Pumodo

Our biggest self-realization was that we were not users of our product. We didn't obsess over it and we didn't love it. We lov

Company: Joost

Select VC Investors: Sequoia Capital, Index Ventures

保持饥饿，不断创新

Joost attracted investment — \$45 million to be exact —

Company: Wesabe

appeared to be the antithesis of YouTube, suspected by

Between the worse data aggregation method and the much higher amount of work Wesabe made you do, it was far easier to have a good experience on Mint, and that good experience came far more

大不尽是优势 Big Is No Guarantee

- 昔日英雄现熊像 - Yesterday's bulls are becoming struggling bears
 - Declining traditional switch/router product sales
 - Lacking competitive security products for emerging environments

Cisco Layoff to Hit 6,000 Workers, Pressure on Chambers?

Juniper Networks Inc. (JNPR) Chief Executive Officer Shaygan Kheradpir is making good on his promise to streamline the company.

The networking-equipment maker is cutting 6 percent of its workforce and ceasing development of products that will result in a smaller, more focused company.

Why Open Innovation Could Be Marissa Mayer's Downfall At Yahoo!

长江后浪推前浪，前浪自大难逃亡

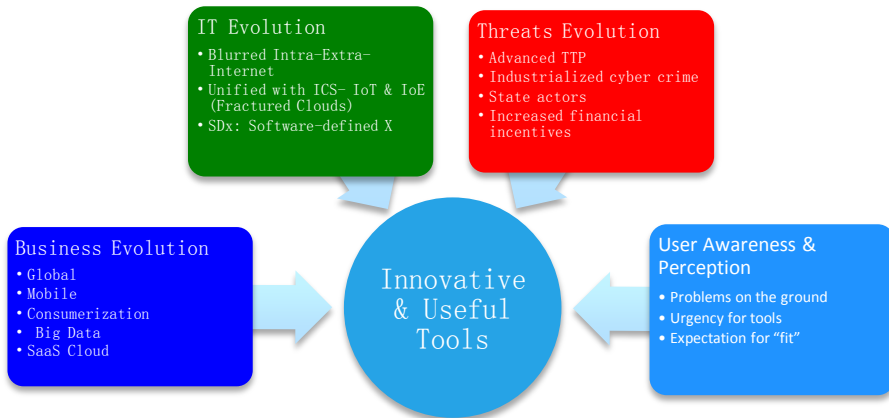
Symantec has undergone a series of leadership changes as the company struggles with a personal-computer slump that has crimped sales of its core antivirus software. While Symantec helped pioneer anti-hacking technologies, it has increasingly found itself out of step with the security industry. Recent data breaches at **Target Corp. (TGT)** and **JPMorgan (JPM)** Chase &

创新制胜 Power Of Innovation

- Bay Area Council Economic Institute & Booz Allen Joint Report 2012
- Three Innovation Strategies
 1. Need seekers: understanding problems & anticipating needs
 2. Market readers: seeing demand trends & catching the wave
 3. Technology drivers: building best tech & looking for market

	Innovation Strategy	Business & Innovation Alignment	Culture for Innovation	Be A Need Seeker	Tech Leader Report To CEO	Continuous Talent Refresh
Silicon Valley Co	89.3%	53.6%	46.4%	46.4%	75%	46%
Overall Survey	80.3%	14.3%	19.2%	27.7%	62.9%	26%

创新需有用 Key Innovation Drivers



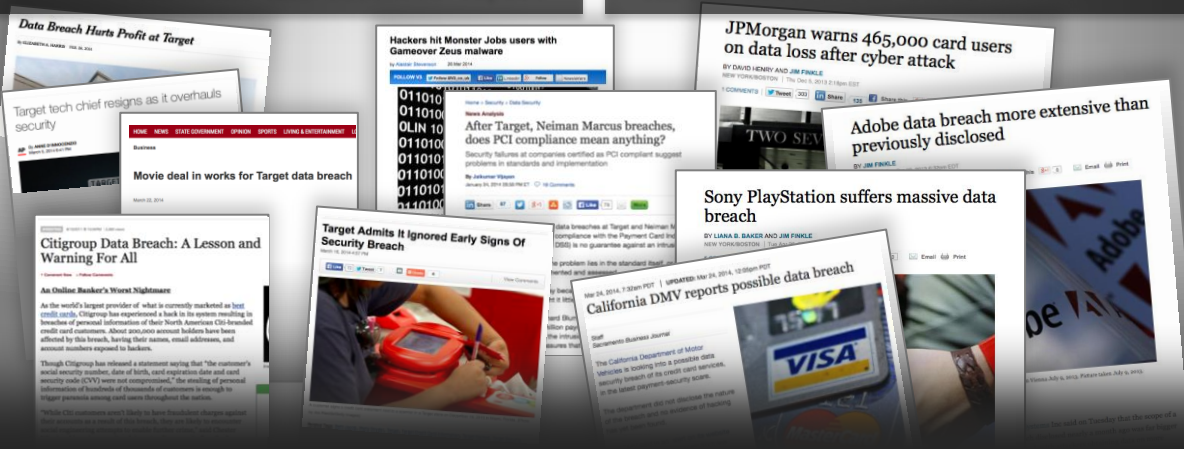
深远影响 Impact Of Security Breaches

Information and IP loss

Brand and reputation loss

Financial and business impact

Threat resolution costs



用户视角IT Perspective Changes



Transformed IT Landscape

IT consumerization & perimeter-less, zero-trust enterprise renders current solutions useless



Impact of Breaches

Crown jewels – intellectual property, customer & business data, reputation, business continuity



New Stakeholder Dynamics

CEO & Board with elevated awareness of business risk, from compliance-driven to risk-driven

大趋势解读 Big Trends

○ Top 8 Security Buzzwords

1. Big Data
2. Machine Learning
3. Behavior Detonation
4. Actionable Intelligence
5. Continuous Monitoring
6. Intelligence Sharing
7. Software Defined X
8. Security Ecosystem

Big Data & Machine Learning

○ Big Data 大数据

○ It is not about

- 哪级干部每周几次公款消费方可支持我不转做大数据？
- How many TB of data, or structured/non-structured

○ It is about

- How long into the past (时间)
- How many sites or how many companies (空间)
- How deep into the business transactions (深度)

○ Machine Learning 机器学习

○ It is not about new SVM or Decision Tree algorithms

○ It is about insights on

- Mapping your problems to suitable algorithms
- Choosing right features for learning

Continuous Monitoring & Mitigation

- Continuous Monitoring 无间断监控
 - Why - watching intrusions is neither necessary nor sufficient for controlling the damage from intrusions
 - It is not about
 - Monitoring just the front doors
 - Using your AV/IDS/IPS/UTM etc.
 - It is about
 - Monitoring all points of traversal, all the time
 - Using all methods available
- Mitigation With Actionable Intelligence 有效动作
 - Full context: what happened whom how, how bad?
 - Ready-to-take actions for attack containment, damage control, future hardening

Behavior Detonation & Intelligence Sharing

- Behavior Detonation 行为施放
 - It is not about
 - Generic sandboxing, or
 - Emulation of a few OS configurations
 - It is about
 - Eliciting software behavior to the extent necessary for detection
 - Matching detonation environments to protected targets
- Intelligence Sharing 情报共享
 - It is not about
 - Botnet CnC servers or SPAM domains
 - It is about
 - Attack campaign: malware, TTP, targets, actors, objectives
 - Propagation trends and proactive counter measures

SDX & Security Ecosystem

- Software-Defined X

- It is not about

- Software defined networks (SDN), software defined storage (SDS)
 - Or, network function virtualization (NFV)

- It is about 长远目光

- Valuing flexibility and scalability over efficiency

- Security Ecosystem

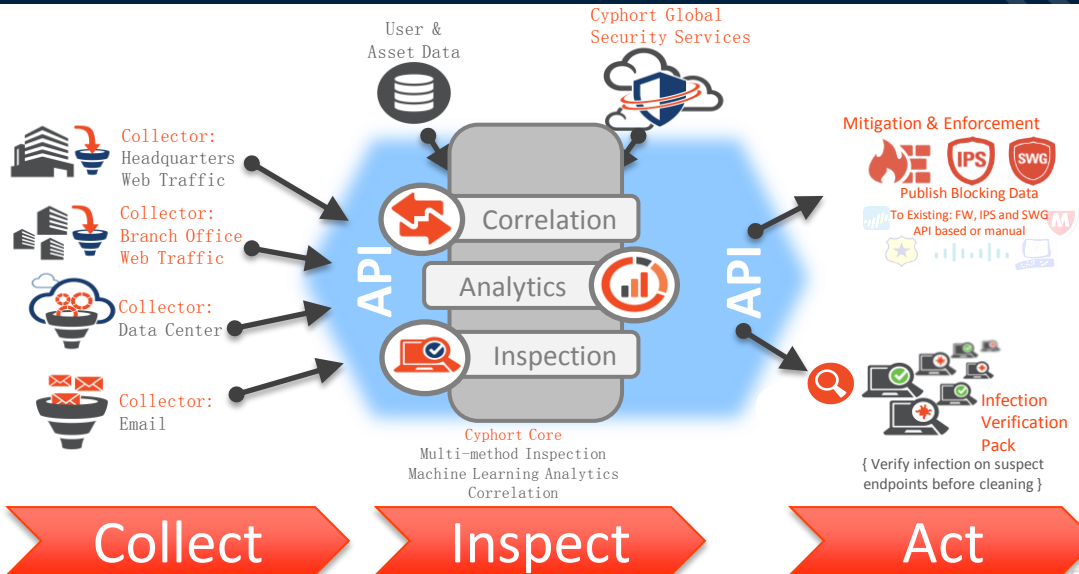
- It is not about worrying vendor's competition anymore

- It is about

- Eliminating the weakest security link 敌人是狡猾的
 - Learning from enemy, unite all the defenders 团结联防

希拉里.克林顿说过，需要全村的人参与才可以养育好一个孩子。我说，需要全部的安全生态系统配合才能有效地抵御现代安全威胁。

Cyphort Architecture



Reduce Your Risk, Prioritize Your Response



Visibility
across
entire attack
surface



Detection
of advanced threats that
matter



Containment
with speed and
automation



Scale
with flexible
deployment

Winning!

Awards &
Recognition

NETWORKWORLD
12 Hot Security Start-Ups


ISAC CONFERENCE
INNOVATION SANDBOX
Top 10 Finalist

Info Security
Products Guide
2014
GLOBAL EXCELLENCE
GRAND
★★★★★

Technology

sgi **box**

 **EVERNOTE**


 **Palantir**

Finance

 **LendingClub**

PROSPER

 **Guardian
Analytics**

JPMorganChase 

Media & Entertainment

NETFLIX

TRIBUNE
MEDIA SERVICES

hulu

Utilities

 **PG&E**

GATX
Rail

Retail



UNDER ARMOUR

ebay

And More...

Fenwick
FENWICK & WEST LLP

CCSD
CLARK COUNTY
SCHOOL DISTRICT



UCSC

IDEO

NETFLIX



“Cyphort’s software-based approach enables us to secure our “elastic perimeter” and provided the deepest insight and richest analytics of all the solutions we tested.”

**MIKE D. KAIL,
VICE PRESIDENT OF OPERATIONS
NETFLIX**



Thank You!

fgong@cyphort.com