安全创业与融资的哪些事

从安全，到大安全

伍海桑博士　志翔科技联合创始人

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018　Beijing·China
（原中国互联网安全大会）


WHAT TO SAY

作为一个大数据安全创业公司
志翔科技为何受到资本青睐？

科幻小说里的“人工智能”离我们有多远?

1997年

IBM“深蓝”战胜了卡斯帕罗夫

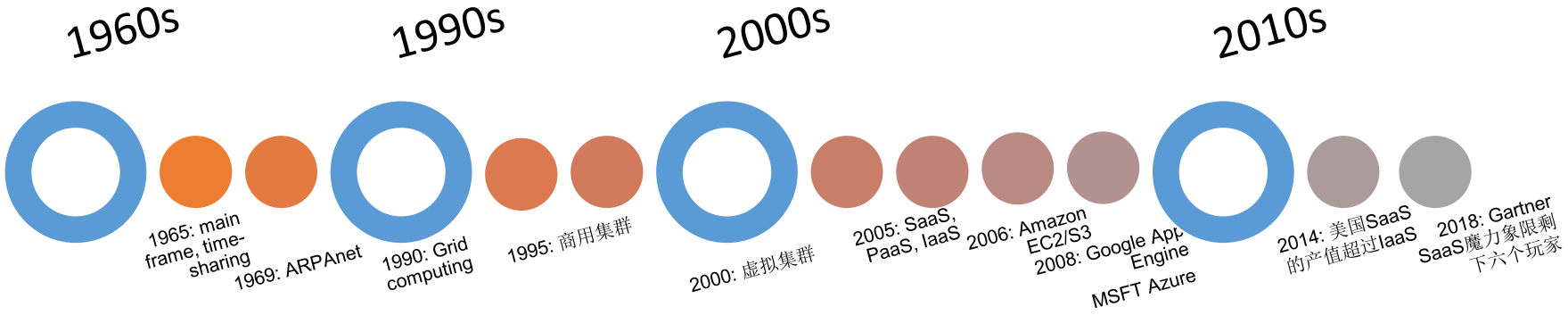
你当时以为，

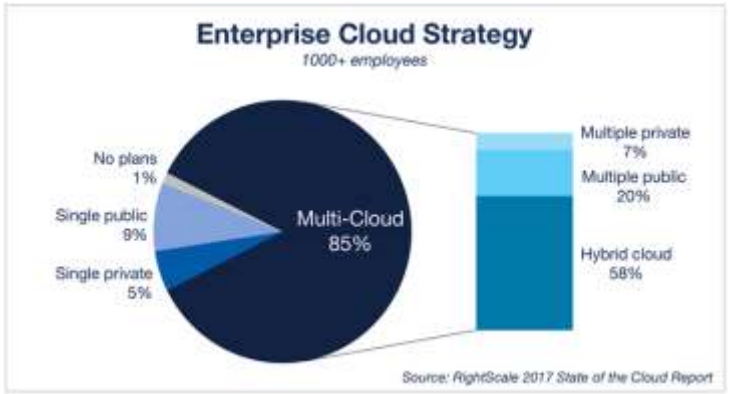
大概2018年，应该会这样

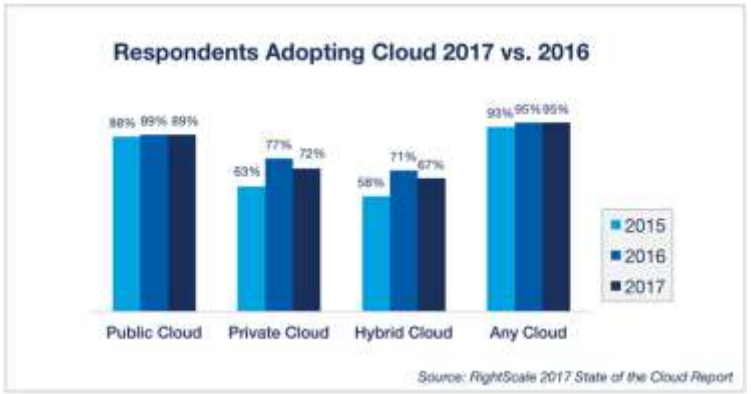
2018年（人工智能诞生68年）

自动驾驶计划：
通用 2018, 福特 2021, 本田 2020, 丰田 2020, 日产 2021, 宝马 2021, 沃尔沃 2021, 特斯拉 2017, Uber ?

云计算离我们有多远?

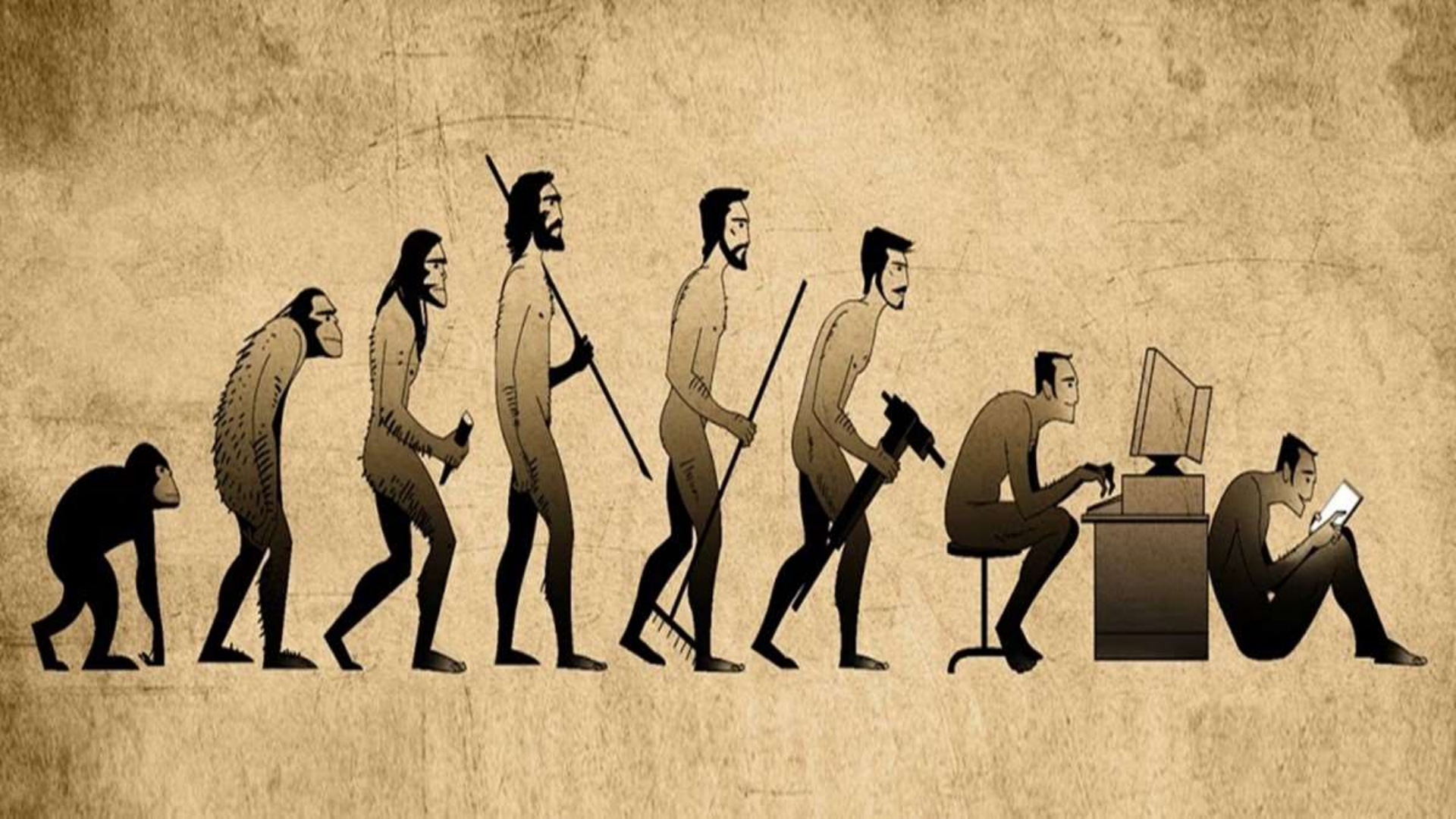






变革往往带来成功的跨界

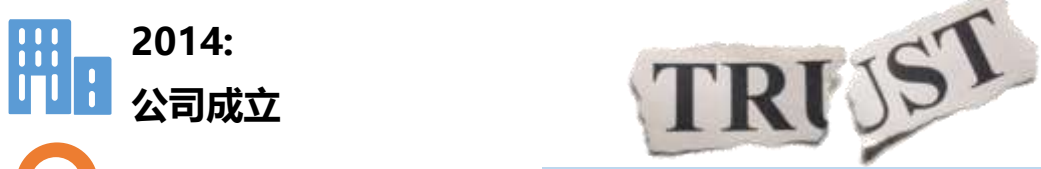
- 安全, Cloud Computing, AI, ML 跨界 =>?
- 颠覆，还是外延传统安全?



志翔的创业之路-2014

2014:

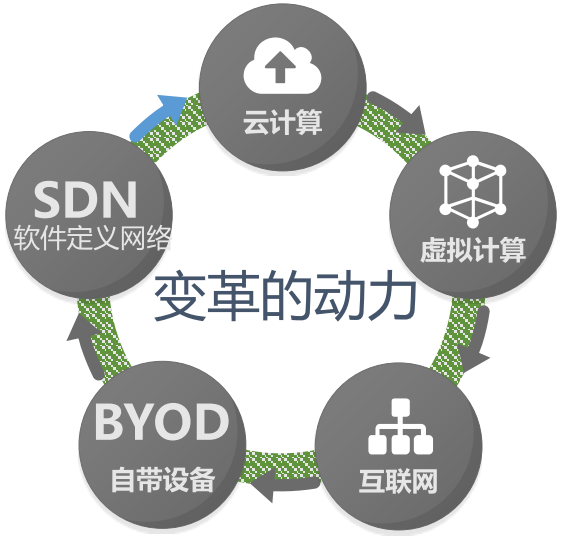
公司成立



企业上云的最大顾虑是安全

一堆清华电子系毕业的中年“创业者”

企业IT生态已经发生巨大变化



安全设施的变化

自建IT系统，物理控制+基于参数的访问控制：网关、防火墙、应用过滤等

基于行为特征和应用特征：IDP、SIEM、 NGFW

正在出现：智能安全、交叉关联的SIEM、持续监控、精准分析

终端变得复杂多样，数据和计算趋向集中（云），安全也要跟随基础设施而变

我国的安全市场规模不大，增速很快

Region	2018 Forecast Spend (US$M)	2018 Forecast Growth
North America	$43,836	+9.0%
Western Europe	$24,128	+7.6%
Mature Asia/Pacific	$14,690	+7.0%
Greater China	$4,287	+14.3%
Emerging Asia/Pacific	$2,739	+11.2%
Latin America	$2,717	+5.0%
Middle East and North Africa	$1,637	+9.4%
Eastern Europe	$1,365	+8.3%
Sub-Saharan Africa	$685	+7.3%
Eurasia	$585	+3.8%

Forecast: Information Security, Worldwide, 2015-2021, 4Q17 Update

国家政策

▶ 保护信息安全是安监部门应承担的社会责任

《中华人民共和国刑法修正案（十）》：

- 有下列情形之一的，处三年以下有期徒刑，拘役或者管制，并处或者单处罚金：
- “（一）致使违法信息大量传播的；
- “（二）致使用户信息泄露，造成严重后果的
- “将刑法第二百五十三条之一修改为：“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。”
- “违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。”
- “窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。
- “单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。”

民生需求

▶ 信息严重滥用的背景下面临严峻的挑战

现状统计：

- 88.8%的人表示曾因个人信息泄露遭遇困扰
- 泄露个人信息最多的机构：电信机构（76.0%）招聘网站和猎头公司（47.0%）各类中介机构（41.9%）市场调查公司（31.9%）金融部门（30.8%）房地产公司（28.3%）教育部门（23.6%）医疗机构（23.2%）交通部门（12.6%）。
- 垃圾短信、电话骚扰、垃圾邮件被视为因个人信息泄露而带来困扰的三大“罪魁祸首”
- 在公众心目中，认为需要立法保护的个人信息中，最多的前三位分别是：电话号码、身份证号和家庭住址
- 98.9%的接收访问的公众认为有必要通过立法保护个人信息

安全事件

▶ 出于经济利益的驱动，来自内部的敏感信息泄漏频频发生，犯罪事件的逐年增多

泄露敏感信息案例：

- 北京某电信运营商内鬼泄密案，涉案的约定债务标的金额高达1087万余元；由于公民个人信息的泄露，导致一起仇杀，一起敲诈勒索等刑事犯罪的发生；三名电信行业“内鬼”与7名“私家侦探”，均被判处有期徒刑2年多至6年不等。
- 国内某电网公司的一个核心业务系统，由于程序内置的数据库连接账号被恶意使用，导致该业务系统敏感数据被篡改达数月之久。由于恶意用户对行为踪迹进行了清理，无法对事故进行溯源。
- 某地公安部门情报信息系统内的敏感信息屡被故意泄漏，却难以对泄漏源和责任人员进行准确定位。
- CSDN、网易、阿里云、圆通快递、南航、保单、孕妇信息等

志翔的创业之路-2015

2014:

公司成立

2015H1:

完成A轮融资

成立南京子公司

2015H2:

第二次搬家

扩容

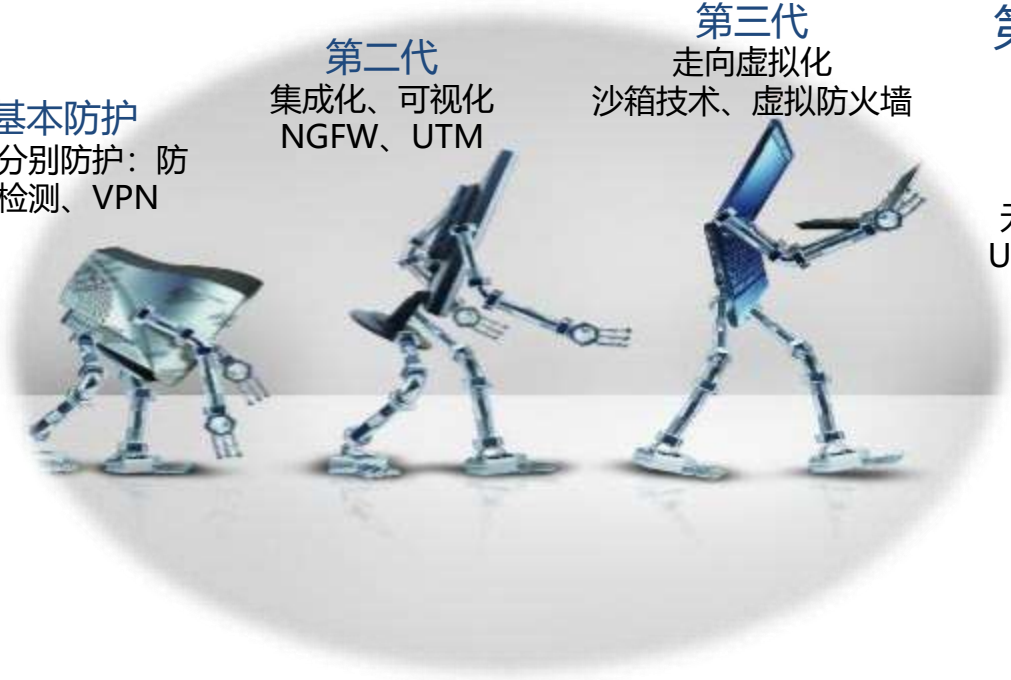
技术变革推动Cybersecurity升级

第〇代—包过滤
在分组层面的简单filter

第一代—基本防护
按网络层次分别防护：防火墙、入侵检测、VPN

第二代
集成化、可视化
NGFW、UTM

第三代
走向虚拟化
沙箱技术、虚拟防火墙



第四代Emerging安全
贴近数据和业务防护
云服务安全
数据采集结合大数据分析
无边界、数据、应用、可视化、
UBA、UEBA、IAM、APT、Zero Day等

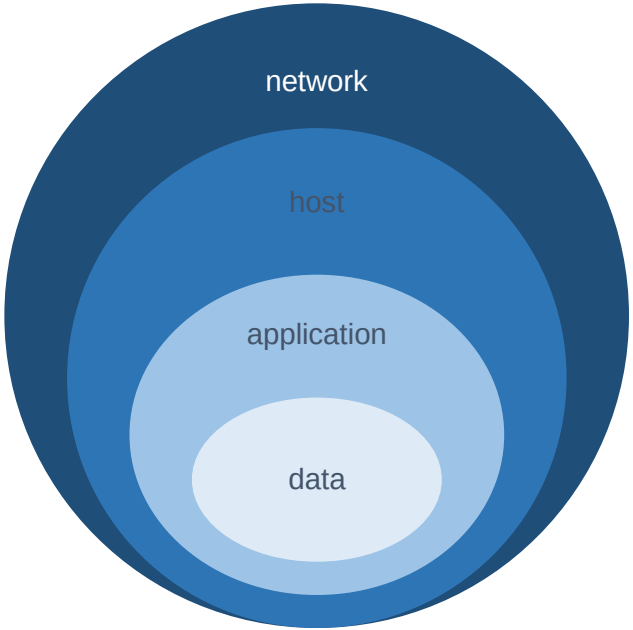
志翔科技 ZSHIELD INC

做大数据安全领导者！

ZERO TRUST SECURITY

志翔认为：大安全需要新理念

- 新中心，新边界：一切安全活动都围绕数据，防火墙不再是边界，身份权限是新边界
- 体系化而非单点防御：基于整体来考虑和设计，从上至下形成体系；数据在哪，机制就到哪
- 行为控制（而非基线补丁策略），擅用数据分析（UEBA, Big Data, ML, VisSec, Actionable Intelligence）



防护纵深的“洋葱”模型

志翔的创业之路-2016

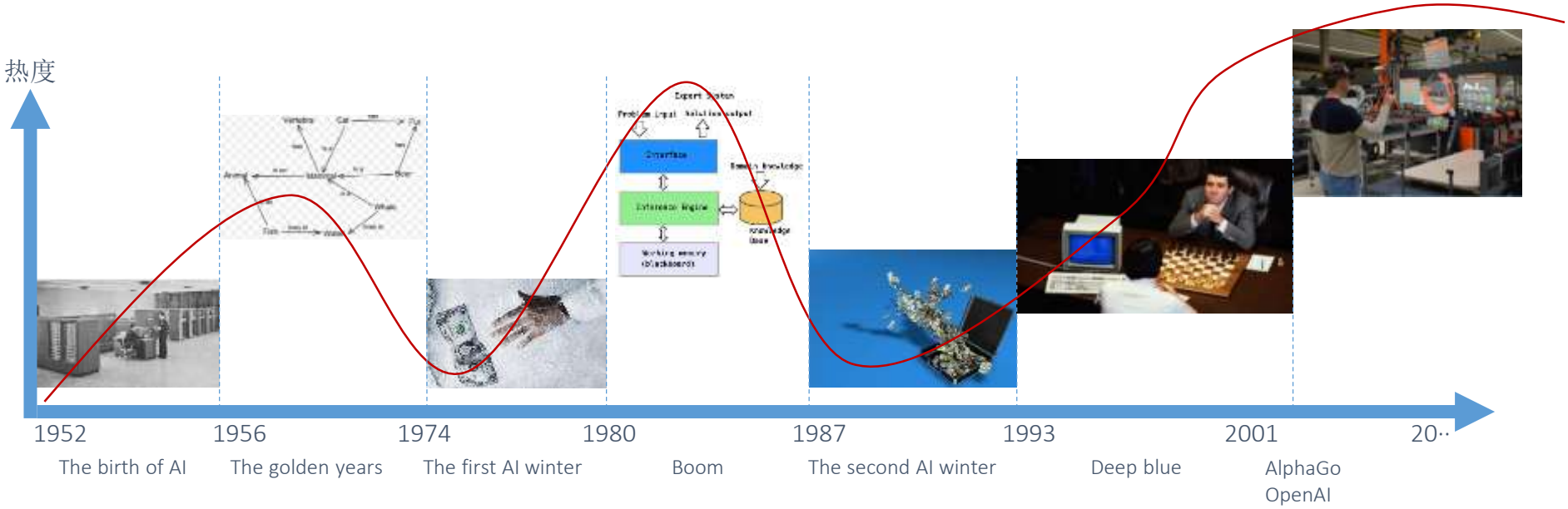
2014:
公司成立

2015:
完成A轮融资
成立南京子公司
第二次搬家扩容

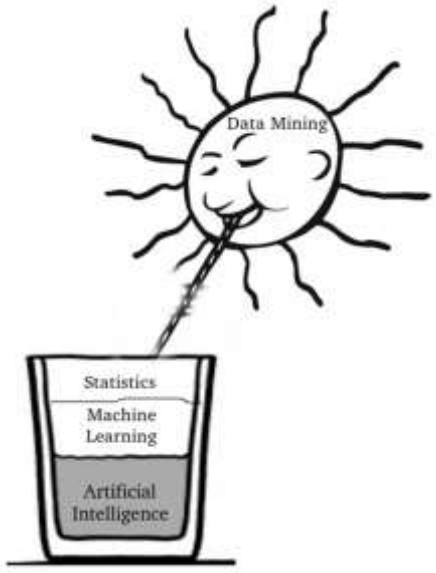
2016:
中国集成电路领域占有率居首

SPREADTRUM 展讯通信
全志科技 Allwinner Technology
Cambricon 寒武纪科技
君正 Ingenic

人工智能的起落兴衰：算力、算法、数据



用“AI”和“大数据分析”提升安全能力



Source：shakthydoss.com

计算机擅长的是计算、规模、海量处理

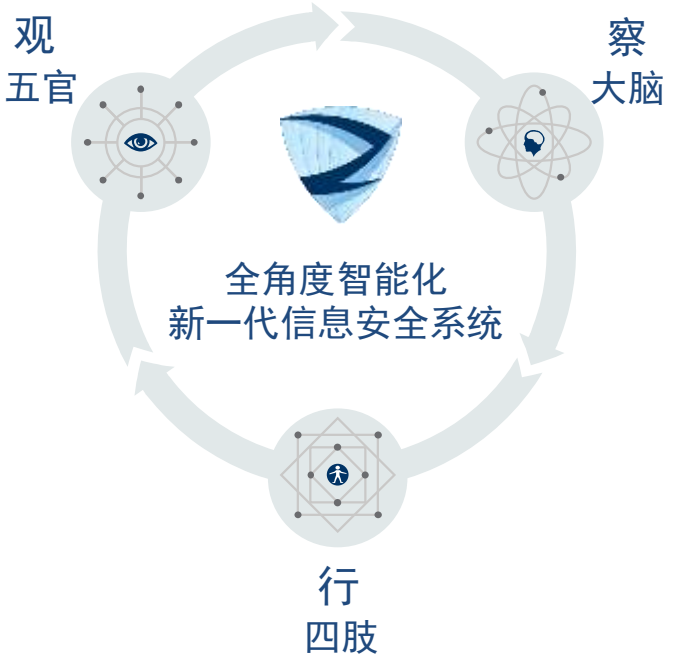
人类擅长的是创造、直觉

Human-machine Synergy

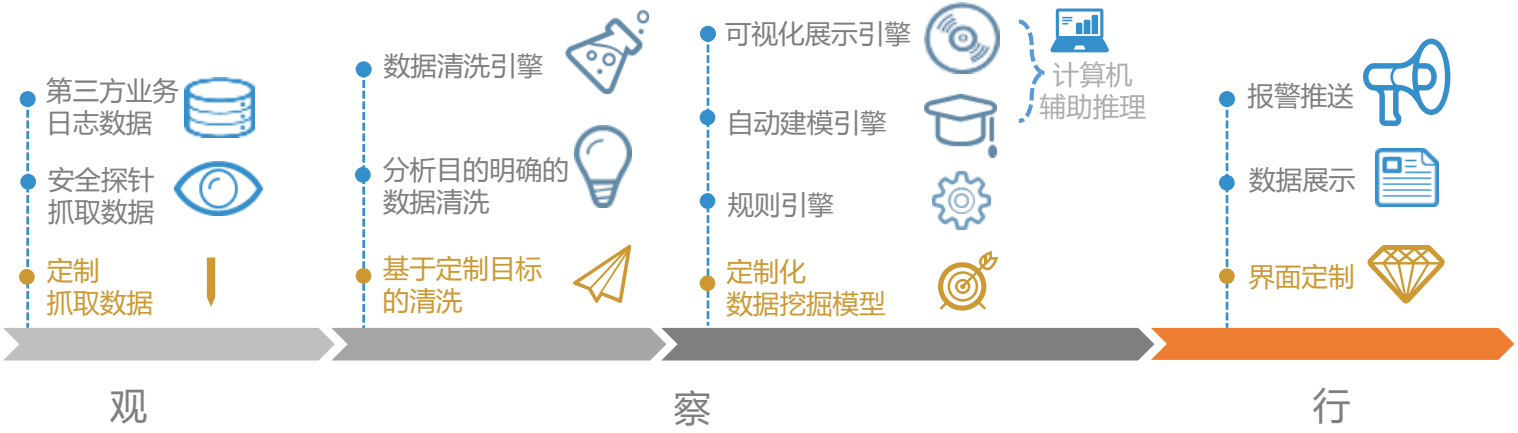
不是让机器自己“发明”创意
而是让人类在机器的帮助下更强大

志翔的技术体系形成：拟人化的安全技术

- “观”—探针和客户端
  - 观察世界和采集信息
  - 不同途径获取多维度数据
- “察”—日志分析
  - 理解行为规则
  - 大数据分析，深度学习，发现违规与不合理行为，提炼更高维度知识
- “行”—至安盾®
  - 从知识到行动：隔离、阻断、报警
- 机器深度学习--指导“观”
  - 针对性数据获取，循环往复不息



在观、察、行中应用人工智能



- 计算机辅助建模
  - AI现状1：机器的推理能力（Reasoning）不及人类，但可辅助人类
  - 对未知事件，深度学习，归纳规律，发现异常
  - 实现了对非结构化和杂凑数据的分析，多维度学习反馈

- 强大的规则引擎
  - AI现状2：机器按规则执行（Rule matching）的效率远优于人类
  - 对已知事件，让机器执行各种复杂规则，进行违规分析
  - 复杂合规系统已经实用，对于千亿条记录，安全系统违规事件反应10分钟之内

志翔的无边界智能安全产品体系

集中式数据保护+安全分析

至安盾™
软硬一体设备，或虚机

分布式数据保护+安全分析

至明安全探针™
分析台 + 终端布点

大数据业务分析和风控

至察盾™
软硬一体设备，或虚机

云服务平台

Security as a Service

物理 Physical → 虚拟 Virtual → 云 Cloud → 形态演进

观

五官：多维度获取数据
一切信息都有用

察

大脑：数据分析深度学习
发现违规异常情报

行

四肢：完善的展示和处理
事前+事中+事后

ZERO TRUST SECURITY

志翔的创业之路-2017

2017H1:

产品进入政府、电力、金融等领域

中国农业银行

IDC Innovator 2017 中国大数据安全

2017H2:

获选IDC 2017中国大数据安全创新者，完成B轮融资

ZERO TRUST SECURITY

从“安全”到“大安全”

全球市场机会

$964亿	$740亿
2018	2017

Garnter

志翔服务行业

政府部门
金融行业
医疗教育
能源电力
通信运营商
高科技企业
汽车、建筑设计

ZERO TRUST SECURITY

志翔的创业之路-2018+

2017H1:

产品进入政府、电力、金融等领域

中国农业银行

2017H2:

获选IDC 2017中国大数据安全创新者，完成B轮融资

2018:

入选 安全牛 AQNIU.COM

中国网络安全企业50强

Future:

ZERO TRUST SECURITY

安全+云计算+分析/ML/AI~大安全

$4190亿美元

预计2019年全球
云计算市场规模

云技术
Cloud technologies

来源：IBM 商业价值研究院

$126亿美元

预计2019年人工智能
市场规模

人工智能
Cognitive/AI

来源：IBM 商业价值研究院

$963亿美元

预计2018年全球
cybersecurity费用

Cybersecurity
spending

来源：Gartner

548家

2017年VC投资的安全
创业企业（467 in 2016）

Cybersecurity
Startups

来源：CB Insights

2018：全球安全市场还处在“战国”时代

传统安全巨头仍居主导地位，但创新企业不断涌现，且发展迅速

- 2017年, IBM总营收800.1亿美元, 同期cybersecurity营收达到24亿美元
- 2017年，Cisco总营收484亿美元，同期安全部门的营收26.5亿美元
- 以上两个公司2014-2017年CyberSecurity收入年增长都在12%以上
- 增长率超过了安全圈的Pure Player: Symantec，Checkpoint
- 安全营收超过了Palo Alto Networks，FireEye，Proofpoint，Fortinet
- 2017年全球安全创业VC投资达到76亿美元——2倍于2016年的38亿美元

RSA的趋势：安全向大安全转变

RSA Conference | Where the world talks security

2013

Security in knowledge

2014

Share. Learn. Secure.

2015

Change: Challenge today's security thinking.

2016

Connect to Protect

2017

Power of Opportunity

2018

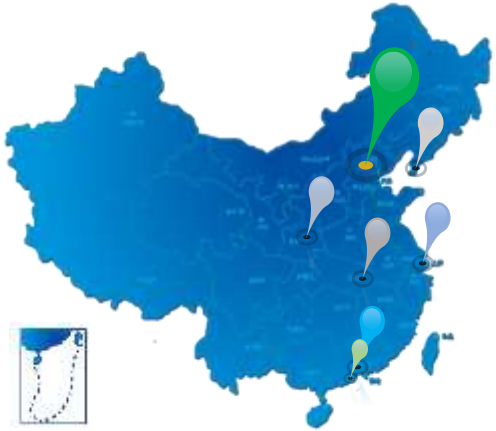
Now Matters

2019

Better.

ZERO TRUST SECURITY

关于志翔



总部：北京中关村

分支：上海、深圳、南京

广州、西安、武汉、大连

IDC Innovator 2017

大数据安全领域创新者

安全牛 AQNIU.COM

2018中国网络安全企业50强

2014年8月由安全和大数据领域多位老兵创立

2015年获A轮投资

2017年获得近亿元B轮投资

核心团队均毕业于清华、CMU等世界名校，多人曾在美国Intel、Juniper等公司担任高管

ZERO TRUST SECURITY