

股票代码：002439



RSA2015

创新沙盒产品技术分析

2015年6月



RSA 2015 概览

大会主题

Change

—Challenges today's security thinking.

**参展厂商
500+**

**参加人员
30000+**

**专题报告
100+**

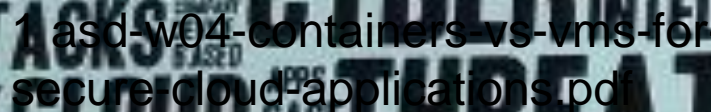
**Keynote
15**

**产业报告
50**

**专题论坛
23**

分析与取证、应用安全与DevOps、工控安全、数据安全与隐私、身份安全、高级威胁、黑客技术、移动安全、云安全与虚拟化、加密、治理/风险/合规、法律等专题

領航
信息安全



威胁情报、云安全、数据失陷、身份识别、移动安全

IT变革

数据中心

云数据中心

传统网络

SDN、无线
物联网、工控互联网

固定办公

移动办公

安全变革

独立

共享合作

硬件

软件与服务

网络安全

应用与数据安全

RSA 创新沙盒10年回顾

10 YEARS | of RSA Conference Innovation Sandbox Contest Winners

2005

SOURCEfire

Raised \$71 million from IPO in 2007

Acquired in 2013 by Cisco for \$2.7 billion

2006

IMPERVA

Raised \$90 million from IPO in 2011

2007

YOGGIE

Raised \$2.8 million within a year of winning ISB

Acquired in 2011 by Cupp

2009

AlertEnterprise!

Raised \$27 million in two rounds of financing

2010

ALTOR

Raised \$16 million in two rounds from four investors

Acquired in 2010 by Juniper Networks

2011

invincea

Raised \$45.5 million from five investors

2012

apthority

Raised \$6.3 million from two investors

2013

remotium

Raised \$1 million within 30 days of winning ISB

2014



Received \$4.6 million within four months of winning ISB

Received \$7.5 million from nine investors

2015

TO BE ANNOUNCED
APRIL 20, 2015

RSA
Conference
2015
San Francisco
April 20-24
Moscone Center

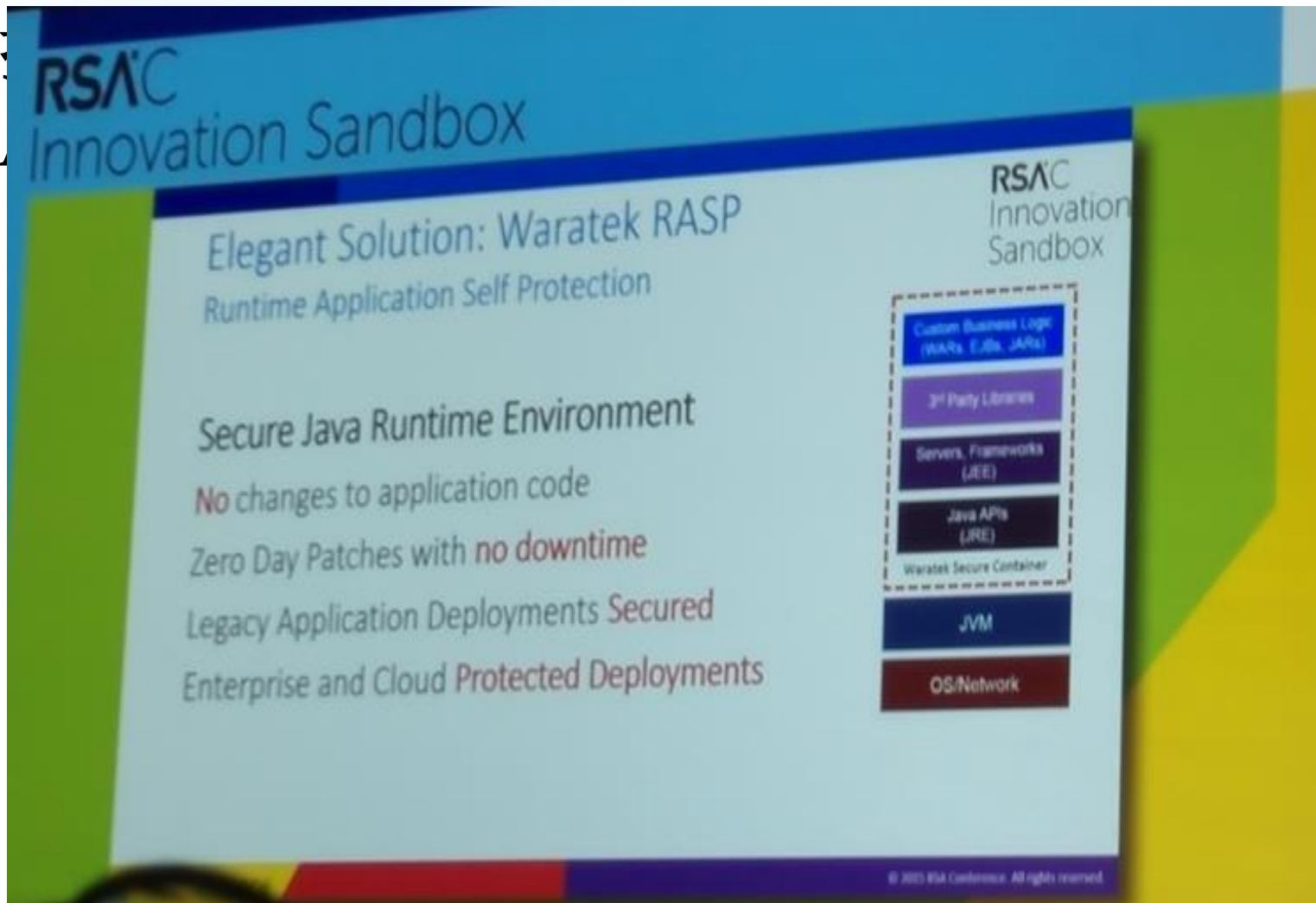
RSA2015创新沙盒入围名单

序号	公司名称	简述
1	bugcrowd	众包安全测试服务管理平台
2	cybereason	终端和大数据相结合的安全威胁检测平台
3	Fortscale	利用机器学习进行日志分析的大数据安全分析平台
4	Nexdefense	面向工控系统的流量可视化及异常检测系统
5	Securitydo	大数据关联查询分析平台
6	Sentinelone	终端安全威胁检测系统
7	ticto	具备可视化屏幕、基于群体识别的身份认证系统
8	Trustinsoft	应用于白盒测试的源代码安全审计系统
9	VECTRA	利用机器学习进行流量分析的大数据安全分析平台
10	waratek	面向 Java 应用的安全防护软件

创新沙盒入围企业分布

- 大数据安全分析：3家
 - Fortscale, Securitydo, VECTRA
- 终端安全：2家
 - cybereason, Sentinelone
- 众包测试平台：bugcrowd
- 工控安全：Nexdefense
- 身份认证：ticto
- 源代码审计：Trustinsoft
- 应用安全：waratek

冠军：Waratek

- 

The image shows a presentation slide for the RSA Innovation Sandbox. The slide features the RSA logo and the title 'Innovation Sandbox'. The main heading is 'Elegant Solution: Waratek RASP', followed by 'Runtime Application Self Protection'. Below this, it lists several benefits: 'Secure Java Runtime Environment', 'No changes to application code', 'Zero Day Patches with no downtime', 'Legacy Application Deployments Secured', and 'Enterprise and Cloud Protected Deployments'. On the right side, there is a diagram of the Waratek Secure Container architecture, showing layers from 'Custom Business Logic (WARs, EJBs, JARs)' down to 'OS/Network'. The diagram includes a dashed box for the 'Waratek Secure Container' which contains '2nd Party Libraries', 'Servers, Frameworks (JEE)', and 'Java APIs (JRE)'. Below this container are the 'JVM' and 'OS/Network' layers.

RSA[®]C
Innovation Sandbox

Elegant Solution: Waratek RASP
Runtime Application Self Protection

Secure Java Runtime Environment
No changes to application code
Zero Day Patches with **no downtime**
Legacy Application Deployments **Secured**
Enterprise and Cloud **Protected Deployments**

RSA[®]C
Innovation
Sandbox

Custom Business Logic
(WARs, EJBs, JARs)

2nd Party Libraries

Servers, Frameworks
(JEE)

Java APIs
(JRE)

Waratek Secure Container

JVM

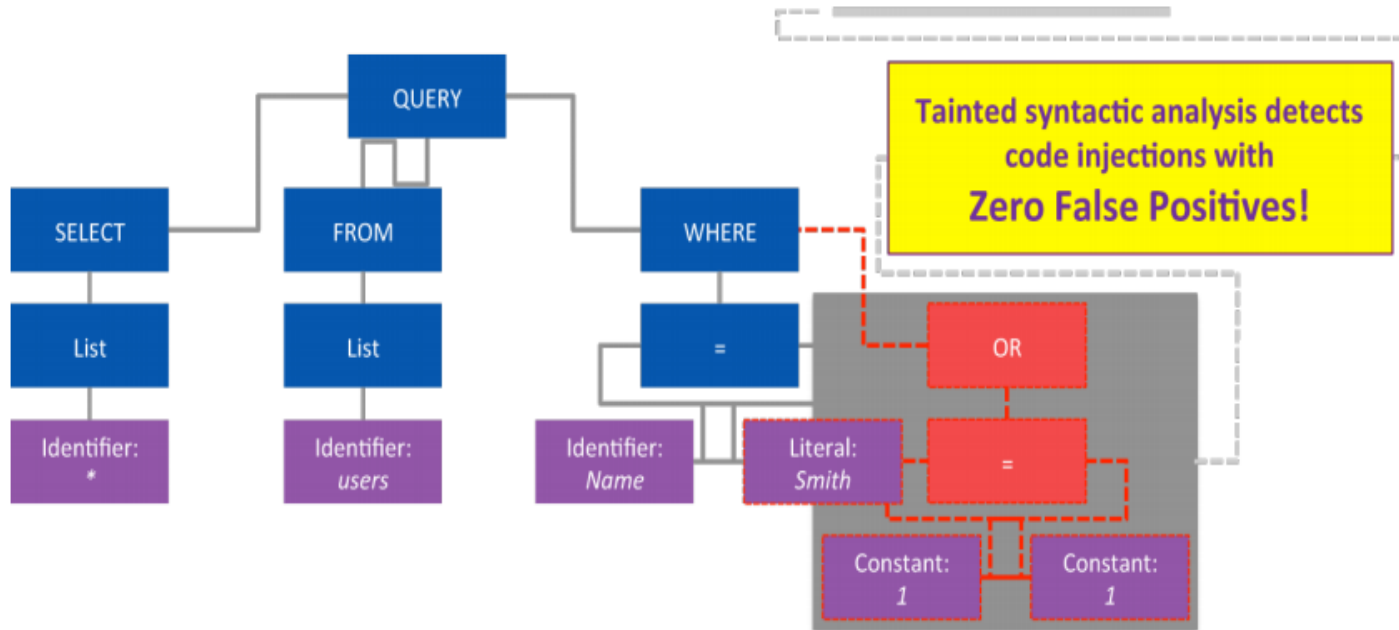
OS/Network

© 2015 RSA Conference. All rights reserved.

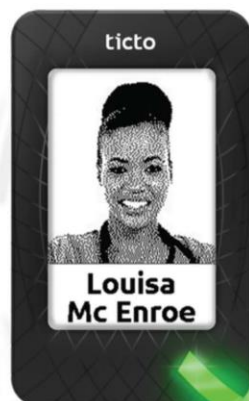
冠军：Waratek

- 基于预定义的规则实现虚拟补丁、0day攻击检测、攻击可视化和取证等功能
- SQL注入检测举例

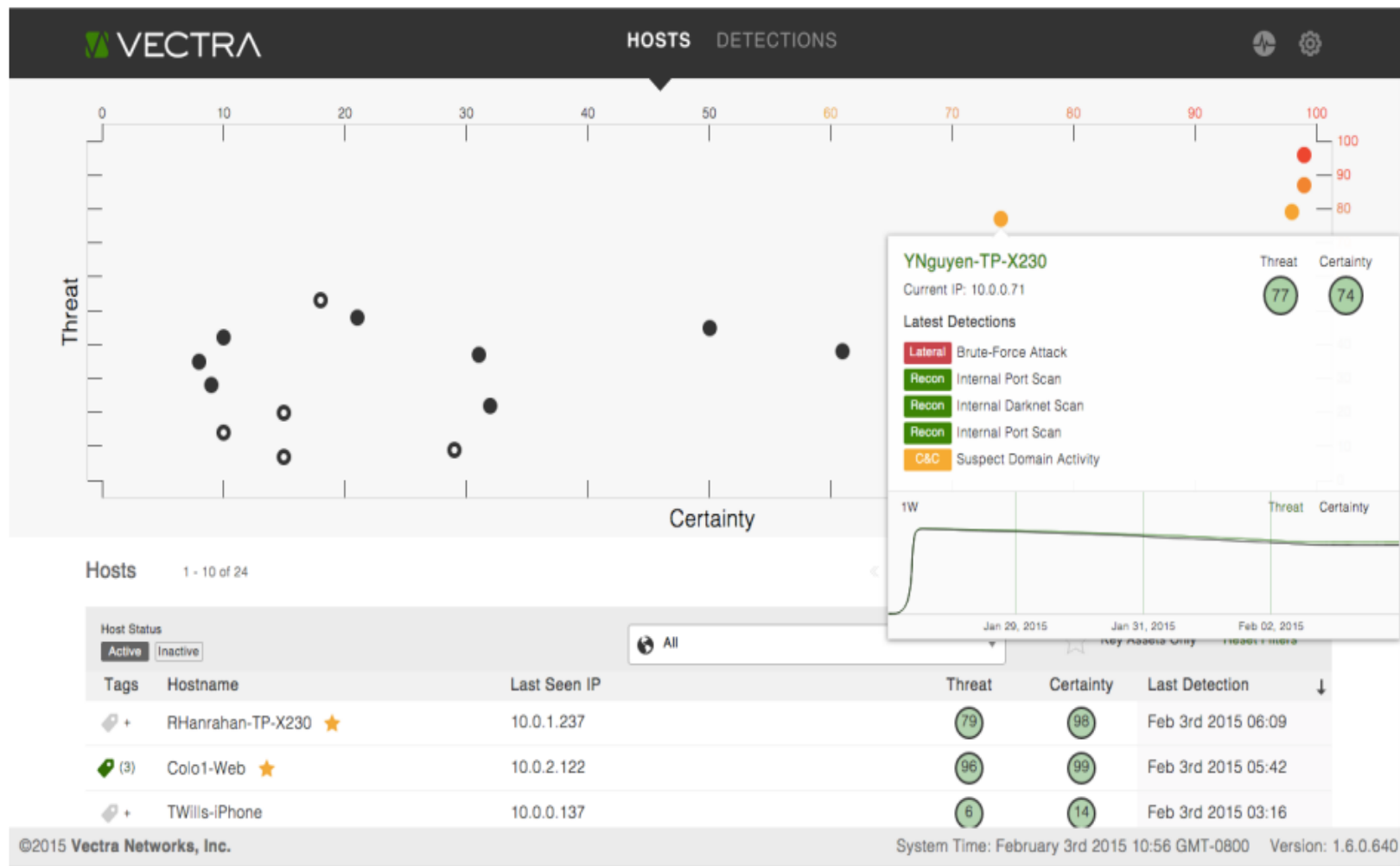
"SELECT * FROM users WHERE Name='Smith' OR 1=1--'";



亚军：Ticto

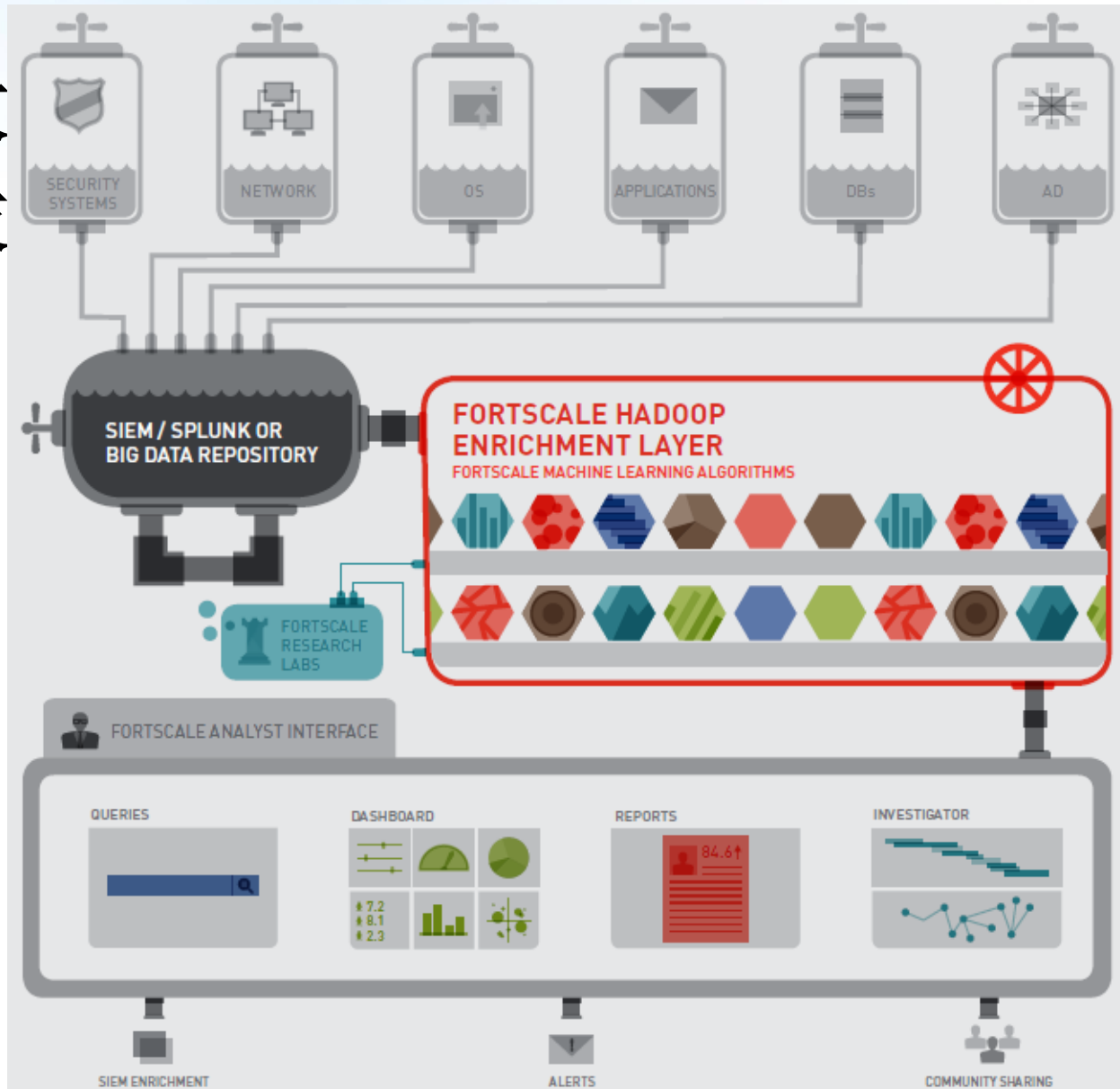


VECTRA: 机器学习+流量分析



FortScale: 机器学习+日志分析

- 数
- 技



仿
并
比



Cybereason: 终端采集+大数据分析

6 Machines

Owner machine



2 users

Owner user



Badoo Media Inc: IEHelper

Known unwanted by hash

Key suspicion



No connections

Incoming connections



6 suspicious

12 neutral

Outgoing connections

updater.exe (26 instances)

Malicious processes



Malicious infection



Malicious external connections

Malop started

updater.exe

Affected resources

Outgoing connections

Malicious activity

Malop detected

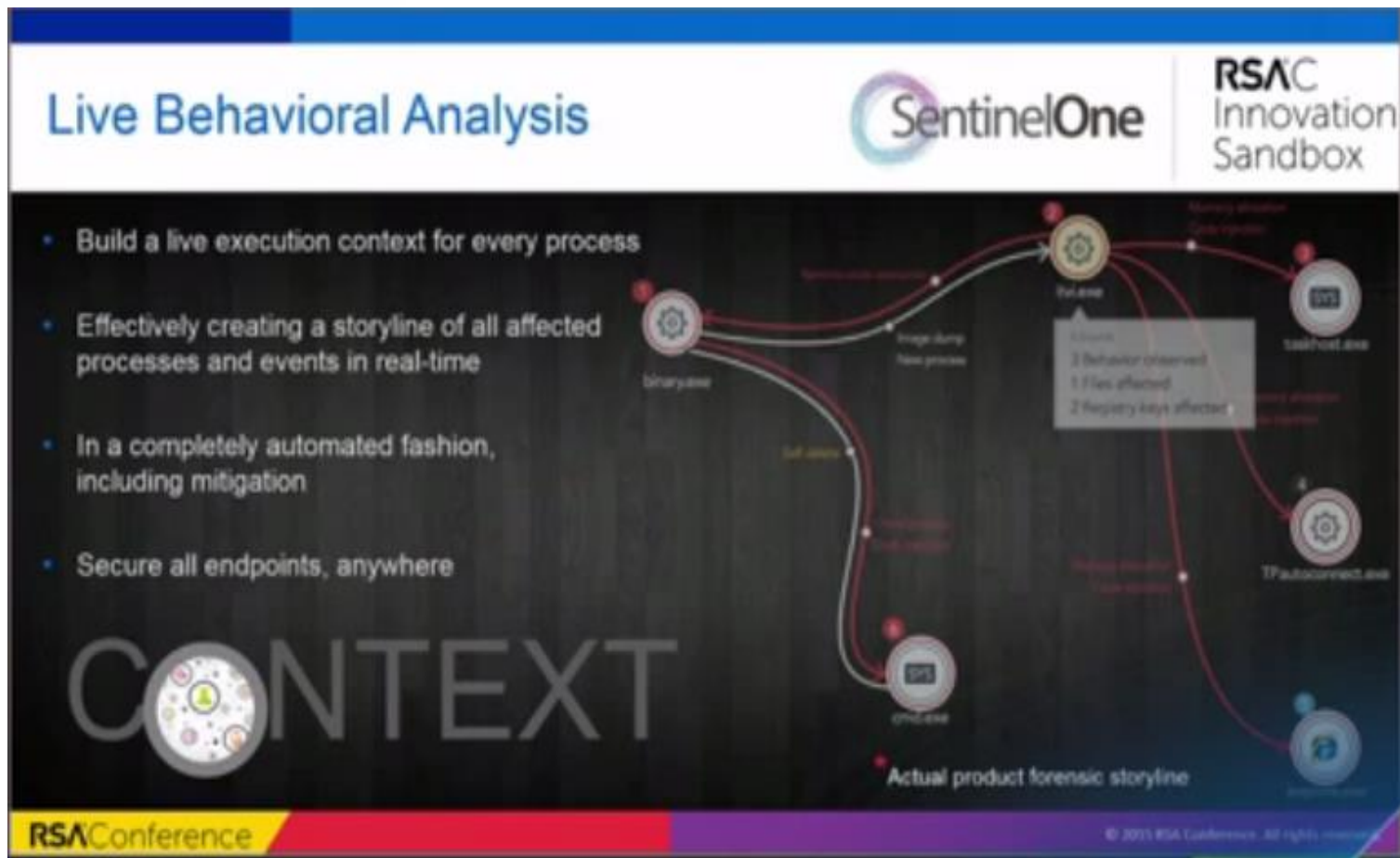
Known Unwanted by Hash

Malicious infection



SentinelOne: 终端检测+云端情报

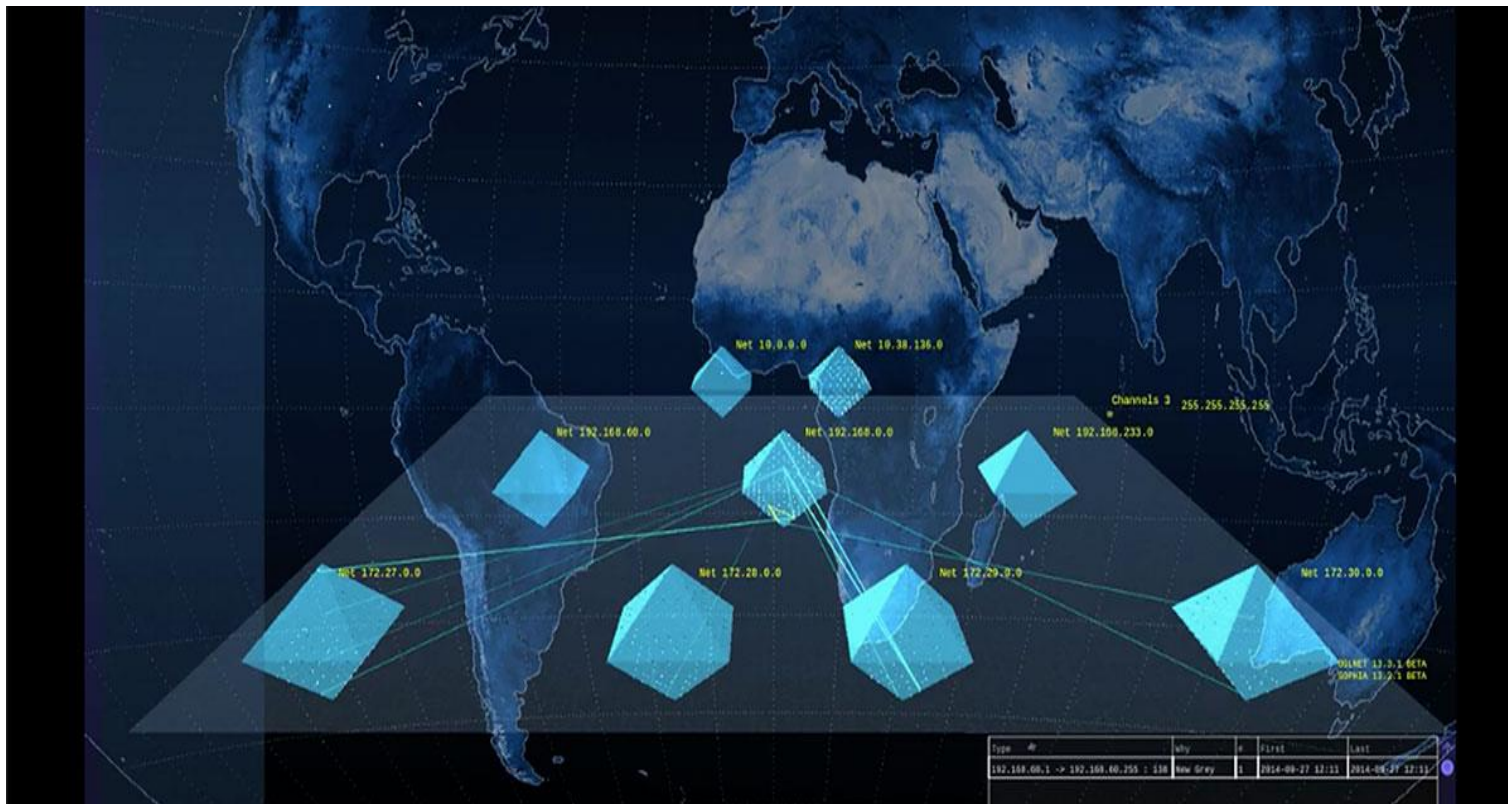
• 技术路线





Nexdefense: 工控安全

- 技术路线：工控IDS+工控FlowEye





Bugcrowd: 众测管理平台

- 技术路线
 - 应用于安全测试服务的众包管理平台
 - 走群众路线：超过16000名安全研究人员利用该平台提供有偿的安全测试服务
- 优势
 - 能力覆盖面广：注册用户擅长的平台、熟悉的应用软件各不相同，比任何一家独立的安全公司都有更全面的安全测试能力
 - 按效果收费：按照检测出的可成功利用的脆弱点数量收费的服务模式

创新沙盒的发展趋势

1. 大数据安全分析是初创公司扎堆的热点领域
2. 基于机器学习的可疑行为检测技术成为研究焦点
3. 从客户环境中采集数据、汇总到云端提炼安全情报，再共享到客户环境中，成为安全情报产生和使用的重要情景
4. 以轻量级代理 + 弹性计算平台的方式提供安全能力，成为初创公司青睐的业务模式，硬件盒子出现的越来越少
5. 众包模式作为一种新兴的生产组织形式，开始出现在网络安全服务中



启明星辰

领航信息安全

谢谢!

