Security Level:

创新，能否带来信息安全的革命？

www.huawei.com

Author/ Email: Author's name/Author's email

Version: V1.0(20YYMMDD)

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

1 无处不是大数据
—大数据对安全业务价值的全面爆发

2014 RSA Innovation Sandbox十大创新公司

RedOwl Analytics

- 提供主动安全分析以减少运作风险，主要服务于金融机构、研究公司、财富500强公司和政府机构等，为其提供尖端的前瞻性安全解决方案，提供大数据分析和调查的新思路。

White Ops

- White Ops 聚焦于检测JavaScript bot，它提供防欺诈和安全解决方案，并在广告界、电子商务和企业商业系统中得到了很好的应用

Bluebox Security

- Bluebox Security 聚焦于企业移动安全，主要针对移动平台的数据保护，致力于对所有应用程序的数据(存储或传输)进行保护，它的保护贯穿于整个移动工作流的所有数据。

Cylance

- 采用了数学方法来进行恶意软件识别，使用了机器学习技术，而非传统的签名和沙盒技术。这项技术可有效地对抗恶意软件、病毒、僵尸和未知的威胁，能够快速部署基于云的服务。

Co3 Systems

- Co3 推出了自动事件响应的四个步骤：准备、评估、管理和报告。通过将这些关键步骤自动化，并基于事件响应的最佳实践、产业架构和合规需求予以报告，能确保降低成本和风险过程的有效、准确和合规。

ThreatStream Inc

- 聚焦于基于SaaS的威胁智能平台，它使用了合作平台来聚合全球、本地和可信任的智慧，分析最终数据，并自动将优化的威胁智能集合到现存的客户系统中。

Skycure

- Skycure 是一个主动的移动安全解决方案，目标是解决新安全威胁，满足客户BYOD使用，并能很好地进行安全保护和控制。

Defense.Net

- 主要提供抗DDoS服务，它能与组织已经部署的抗DDoS架构进行联动，便在多数复杂攻击发生时保持业务连续性。它主要是针对组织在抗DDoS解决方案中面临的“集中风险”。

Light Cyber

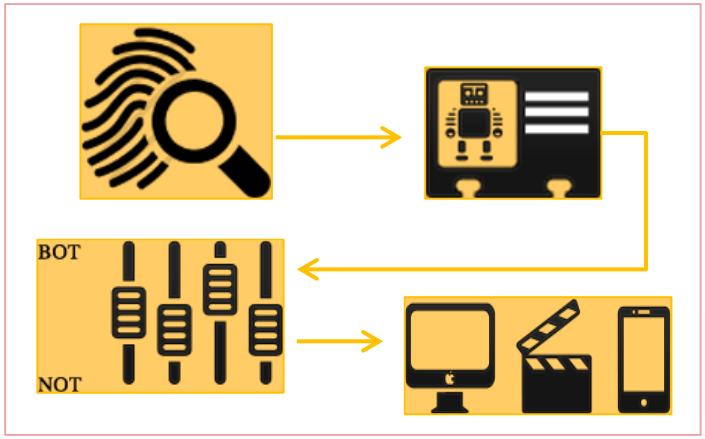
- 为组织提供前瞻性的漏洞检测方案，以保护它们免受有目标的威胁。通过分析网络和端点信息，描述网络用户和设备中的常见行为，通过对恶意行为检测并提供早期预警，在破坏发生前对抗攻击。

Cyphort

- 提供高级威胁防御平台，它能检测并分析下一代威胁和高级恶意软件，提供可追溯的、 有关联的智能信息，以此使得安全团队得以更快更高效地响应

Source: 51CTO

White Ops—基于大数据分析的在线防欺诈保护



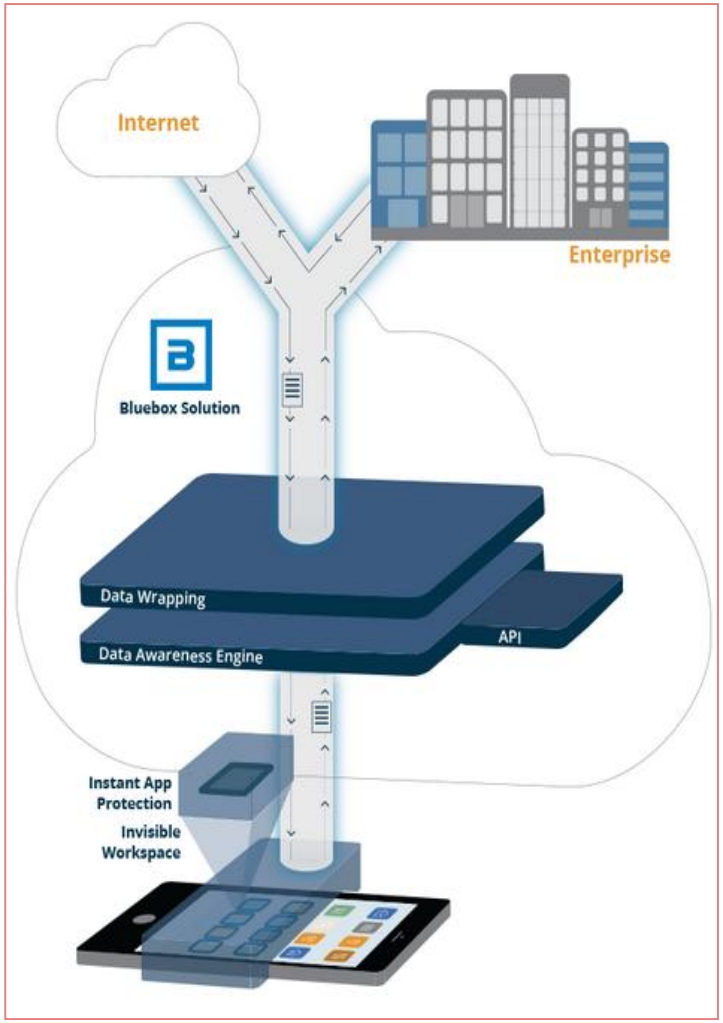
公司定位：

- 基于web的在线欺骗检测和保护，判断流量是人为正常流量还是僵尸代理产生的垃圾流量，服务于广告、电子商务和企业商务系统等在线企业

功能特性：

- 在客户端插入JavaScript脚本，通过把会话参数传送到大数据后台进行分析，后台可以在50毫秒之内分析并确定某次会话是人为的还是僵尸/恶意自动产生
- 后台建立了大数据分析平台，采用了signal intelligence和side channel 攻击分析技术，可以有效判定某次广告点击和电子商务交易的实际情况，帮助客户直观判断网络流量行为
- 构建了针对网络流量的判定处理流程：detect->report->prevent->feedback

Bluebox ：基于大数据(云)的移动应用安全保护



公司定位：

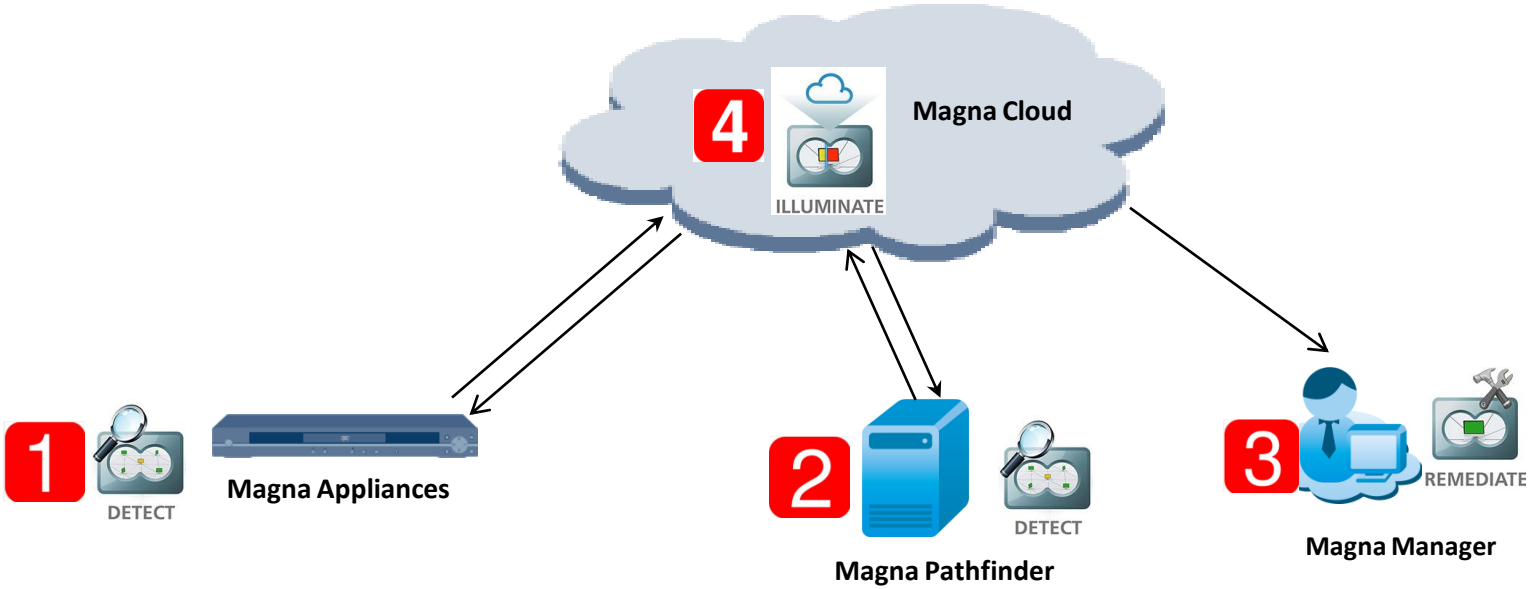
基于云的企业办公安全解决方案提供商

功能特性：

- 在移动终端安装透明APP，通过重定向，所有被保护的企业移动数据会流经BlueBox云数据平台安全管理
- 受保护的终端APP不需要开发SDK，可以按需保护移动终端的各种APP，安全策略可以动态配置和调整
- 客户端提供Invisible Workspace安全沙箱技术，把企业数据存放在IW中，客户端利用data awareness engine标识自动加密和解密企业数据
- 企业通过Bluebox大数据平台，可以跟踪了解企业数据的各种使用情况及数据流向情况，分析Data在移动终端、App或网络中流动的安全情况，保持数据可视化
- 构建以大数据平台为中心的安全保护能力，在Bluebox大数据平台网关中构建了基于数据的自学习保护算法
- 非IW内的数据没有任何管控，保护了用户的隐私，使得终端用户有更好的感受

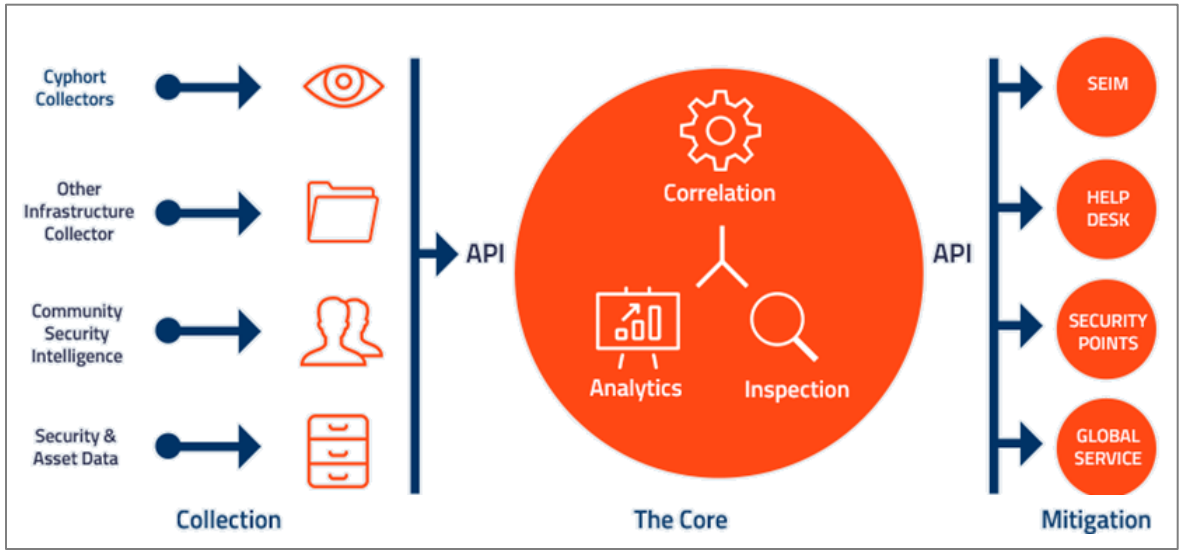
LightCyber—基于大数据的APT威胁检测和防护

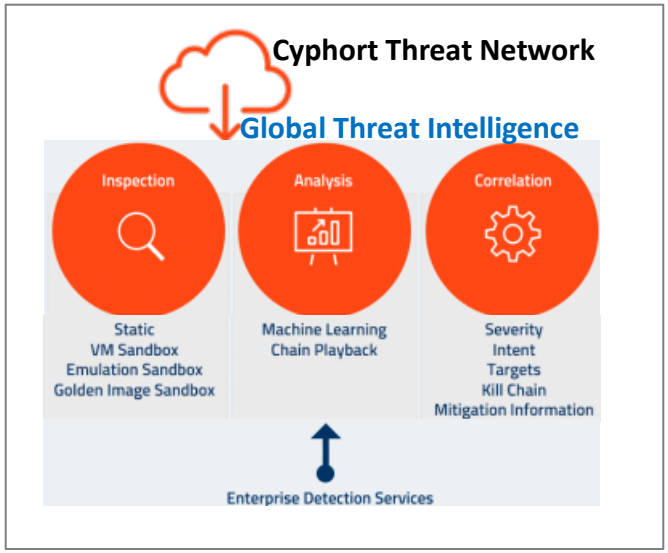
定位：第一家采用大数据针对网络和端点进行APT攻击防护的公司



1 Appliance:	2 Pathfinders	3 Manager	4 Cloud
检测网络内部的流量，采用Netflow、IPFIX、SFLOW，iFlow等采集骨干交换机Span端口的流量，并对流量进行安全检测和防护，可疑流量上报到Cloud上	采用无代理技术扫描可疑的已授权管理的终端电脑，可以检查文件、进程、可执行文件、注册表，探寻可疑根因，检测已知和未知的威胁（检出率90%多）	管理Appliance和pathfinder的安全配置，提供Appliance和pathfinder的安全策略管理，并提供安全修复建议	通过大数据技术，不断对威胁检测算法进行调优，并把威胁检测算法（非签名）自动下载到 Appliances和Pathfinder上，实现云和端的最先进协同处理

Cyphort—基于大数据的集成威胁检测技术





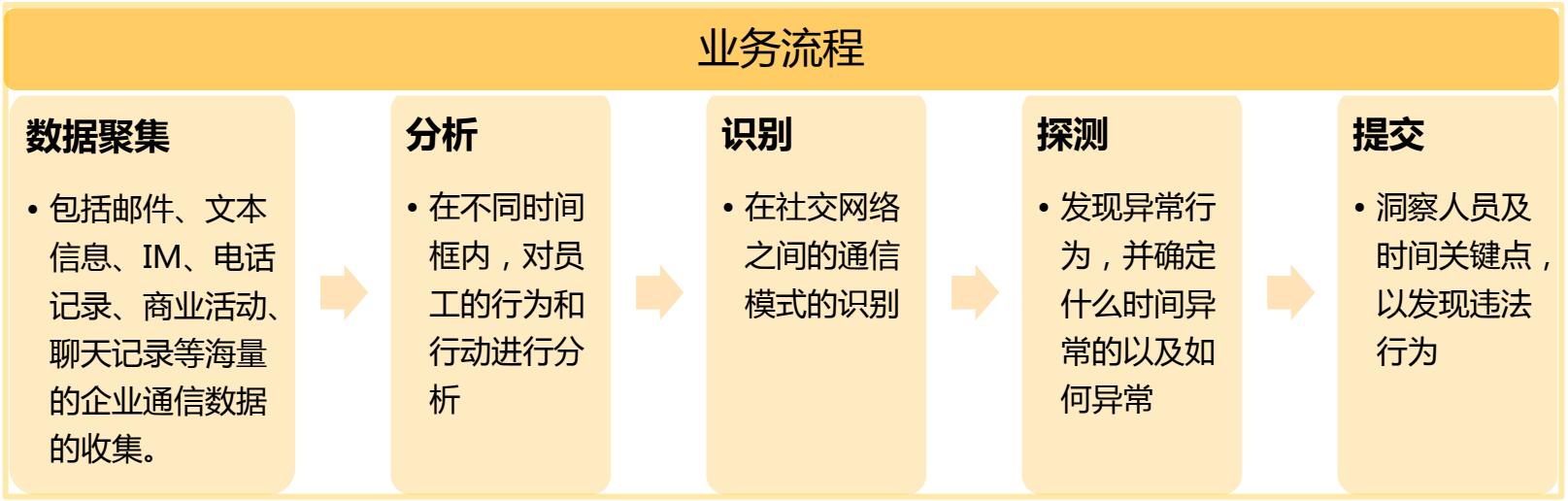
公司定位：

- 基于精准威胁检测分析的APT防护公司

功能特性：

- 通过在Internet出口部署软件形态的探针，采集可疑对象的网络流量及关联元数据，并传输至集中部署在Core上的威胁检测组件进行分析
- 在威胁检测组件中，采用了静态沙箱、VM沙箱、模拟沙箱、Golden Image沙箱等多种威胁检测技术，并辅以机器学习、Chain-Playback等高级威胁分析技术，进行全方位的威胁分析
- 在Core中构建大数据分析平台，采用大数据关联分析方法，将“网络行为”、“威胁检测、分析的结果”关联起来，验证恶意软件、威胁感染程度，提供环节威胁的手段与方法
- 支持开放的API架构，Core提供分布式部署能力，十分易于和现有的第三方解决方案进行整合

RedOwl—基于大数据的行为安全分析



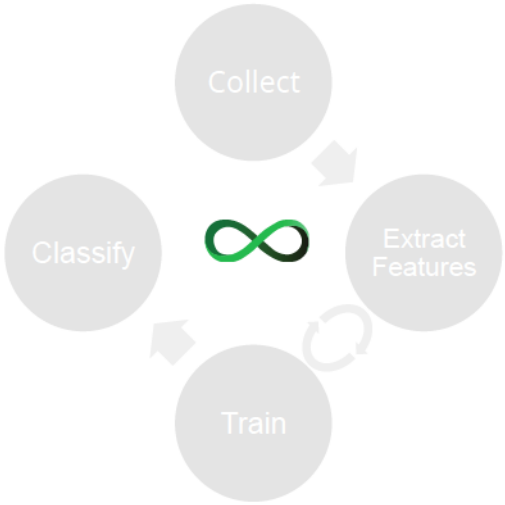
公司定位：

- 基于主观行为分析的大数据安全公司，提供主动安全分析以减少管理风险，提供云服务方式

功能特性：

- 对组织效率、管理文化、沟通交流等员工行为进行大数据智能分析，以改进公司的管理效率
- 基于推论统计学和社交网络架构搭建模型，采用基于Hadoop的大数据平台，并支持获取企业应用软件及第三方平台的数据，并可通过API向外开放所有功能和数据
- 采用元数据和推论统计学算法分析人的行为和动作、以工作流形式来提升电子发现的手段，包括email、text、voice、chat和SNS等，聚焦于对不当行为的早期发现，并通过行为预测算法，智能的自动扩展到早先未覆盖的方式

Cylance—基于大数据的新一代威胁检测引擎



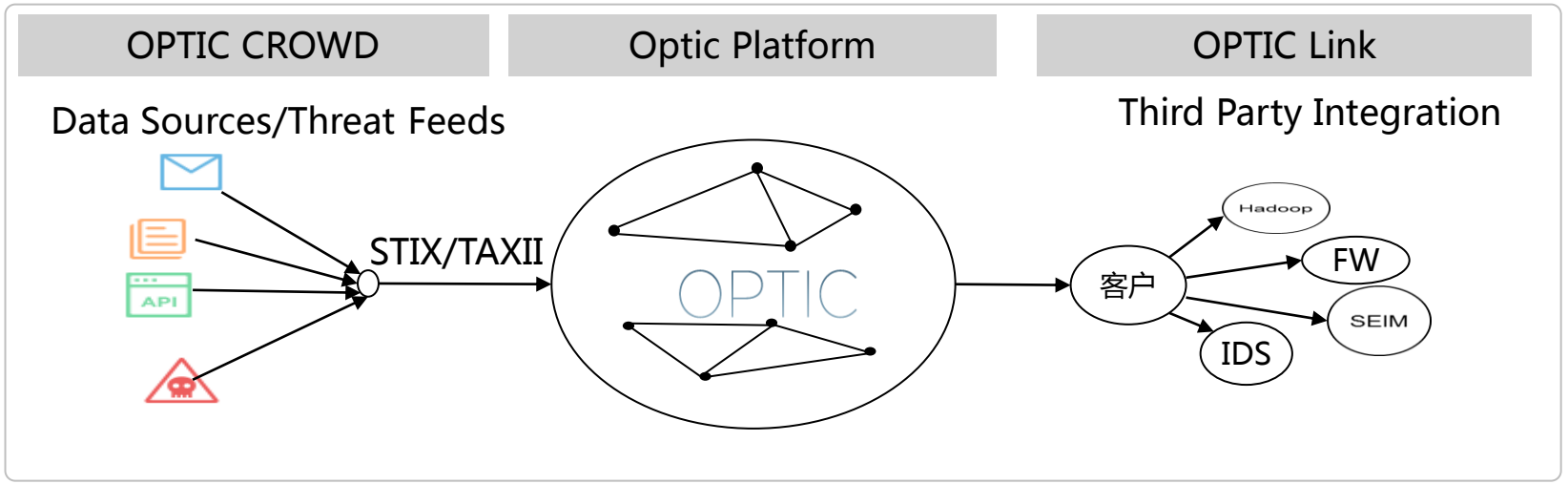
公司定位：

- 提供新一代威胁检测引擎，为关键基础设施，嵌入式系统，企业提供下一代APT防护服务

功能特性：

- 针对APT攻击事件发生之前进行预判并采取响应，重点保护基础设施，嵌入式设备以及重点企业
- 基于大数据平台实现机器自学习和攻击行为的大数据挖掘，利用数学算法实现APT攻击的预判。
- 机器学习侧重于在攻击预测的基础上，基于历史数据和当前行为进行算法预判，数据挖掘的重点是针对未知性质数据的发现，也能有效地识别新恶意软件及未来变种
- 通过大数据平台支撑Infinite威胁检测引擎，可以针对企业终端保护，并可与企业SOC结合强化检测

Threatstream—基于大数据的安全情报平台



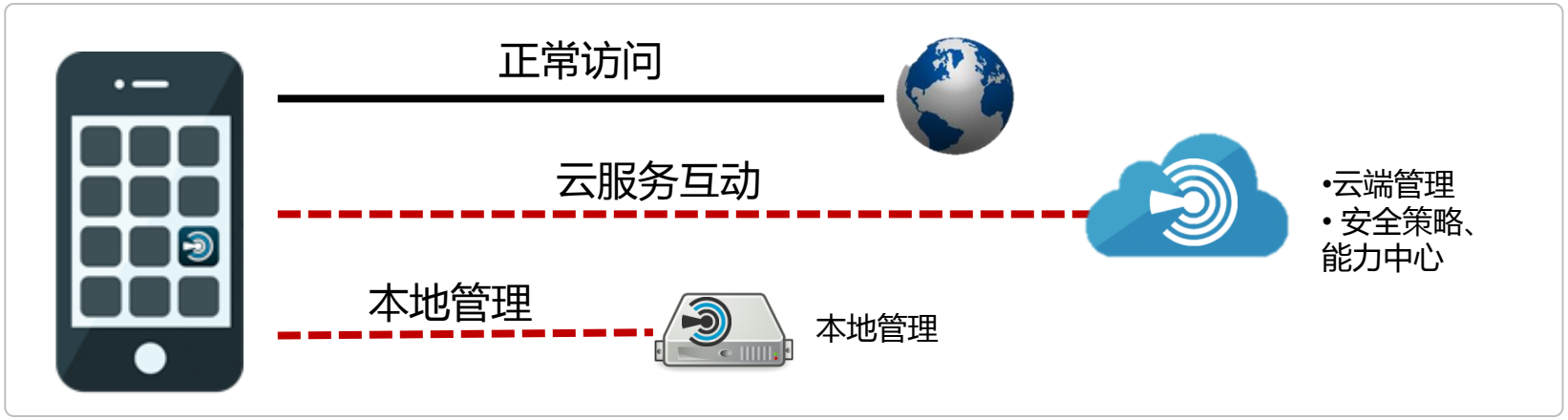
公司定位：

- 构建基于SaaS的威胁智能平台，使用了合作平台来聚合全球、本地和可信任的智慧，分析最终数据，并自动将优化的威胁智能集合到现存的客户系统中

功能特性：

- 广泛获取各种安全威胁情报，情报来源于蜜罐采集、竞争对手、TOR代理、IRC等途径
- 通过独特的机器学习算法来整理并定义威胁情报，基于获取的源信息按照相关性、语义判断、威胁程度等，构建全球最大和最多样化的威胁指标数据集，转化为可操作的威胁情报
- 构建的威胁信息可以与提供到现有的安全架构中，目前已经能够支持ArcSight、Splunk、Sourcefire、PaloAlto等几十种安全产品

Skycure：基于云的移动安全保护



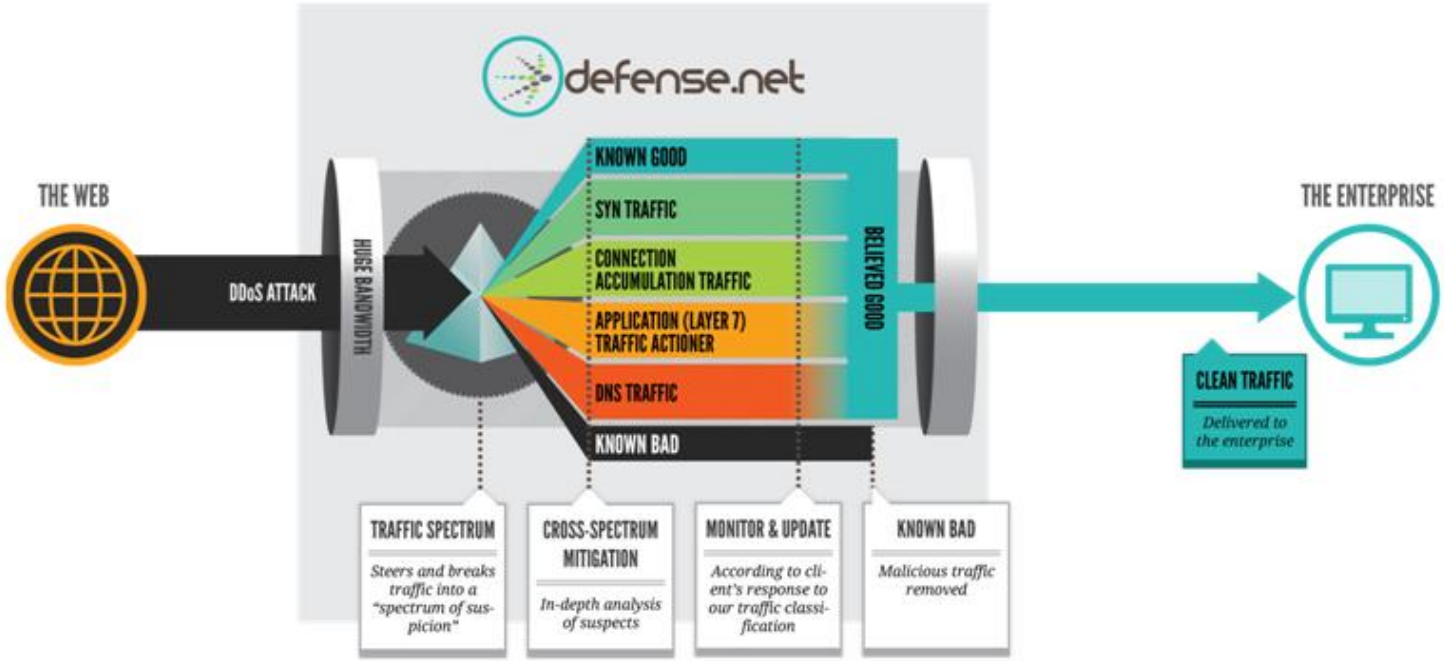
定位

- 提供主动防护的移动安全解决方案，针对新的未知安全威胁的保护

功能特性：

- 建立蜜罐系统，主动探测针对移动终端和无线网络的攻击，进行网络攻击行为分析，支持iOS恶意Profiles检测以及Wi-Fi Attacks检测
- 收集终端用户自动产生的各种知识，并在云端采用大数据平台进行学习分析，并定时进行安全策略更新以及提供按需保护
- 采用SaaS以及On premise的运营模式

Defense.net—基于SaaS的Anti-Ddos服务



公司定位：

- 针对企业组织以SaaS安全服务的模式提供抗DDoS保护

功能特性：

- 采用SaaS或者CDN模式，通过修改BGP或者DNS实现就近部署防控
- 通过Traffic Spectrum(流量光谱)，将各种流量精确分拣出来，不同类型的攻击流量送到几百个不同的攻击缓解子系统中进行清洗，并将清洗后的的流量送给用户
- 利用云和大数据平台，实现全软件化的DDos处理，通过SaaS模式部署，支持所有协议端口
- 基于学习模式自动判断可疑的攻击流量，减少通过人工分析并干预的时间

Co3 Systems：基于云的安全事件响应自动化

公司定位：

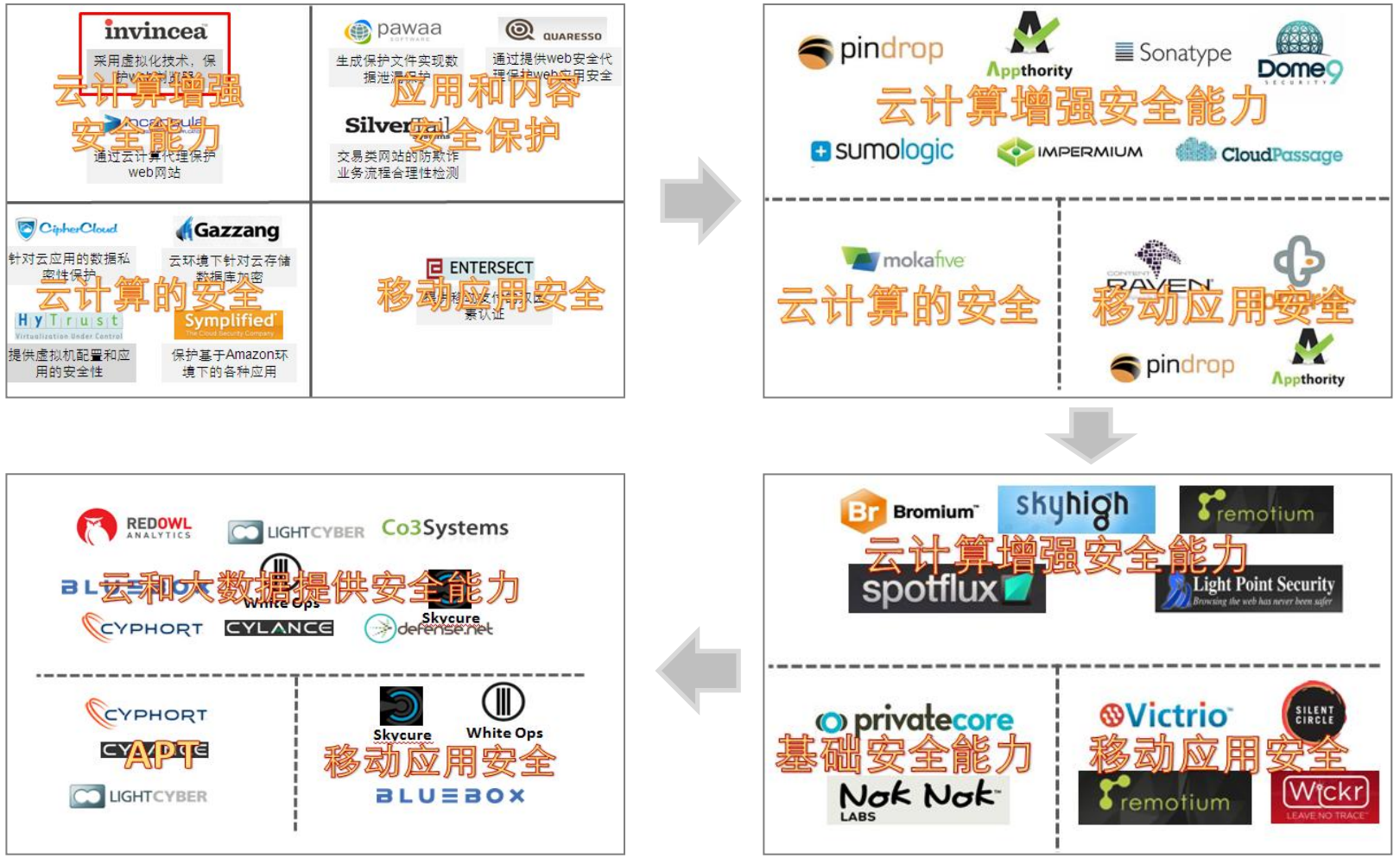
- 针对企业提供自动化的应急事件响应服务（包括安全事件和隐私保护）

功能特性：

- 基于其云平台搭建的知识体系实现安全事件响应的自动化，包含四个处理步骤：准备、评估、管理、报告
- 核心的知识架构基于行业最佳实践、行业安全标准、合规要求、监管要求等构建，满足制度需求
- 提供的响应服务内容包括安全事件响应和隐私侵犯响应两部分，可针对侵犯隐私、恶意软件爆发、系统入侵、DDoS攻击等实现 自动化事件响应
- 目前主要以云SaaS服务模式提供自动化响应，已有数千客户

2 安全创新的演进和未来

安全创新方向的演进


2011
invincea
采用虚拟化技术，保护web应用服务器
pawaa
生成保护文件实现数据泄漏保护
QUARESSO
通过提供web安全代理保护web应用安全
通过云计算代理保护web网站
交易类网站的防欺诈业务流程合理性检测
云计算增强安全能力
应用和内容安全保护
CipherCloud
针对云应用的数据私密性保护
Gazzang
云环境下针对云存储数据库加密
HyTrust
提供虚拟机配置和应用的安全性
Symplified
保护基于Amazon环境下的各种应用
ENTERSECT
云计算的安全
移动应用安全
2012
pindrop
Appthority
Sonatype
Dome9
云计算增强安全能力
sumologic
IMPERMIUM
CloudPassage
mokafive
云计算的安全
RAVEN
移动应用安全
pindrop
Appthority
2013
Bromium
skyhigh
remotium
云计算增强安全能力
spotflux
Light Point Security
privatecore
基础安全能力
Victrio
SILENT CIRCLE
移动应用安全
Nok Nok LABS
remotium
Wickr
2014
REDOWL ANALYTICS
LIGHTCYBER
Co3Systems
BLUEBOX
White Ops
云和大数据提供安全能力
CYPHORT
CYLANCE
Skycure
defense.net
CYPHORT
CYAPT
LIGHTCYBER
Skycure
White Ops
移动应用安全
BLUEBOX

总结：未来安全业务创新四个关键要素

强调长期攻击危害

APT攻击使得针对安全防护由实时性向精准性和持续性发展

强调软件分析能力

软件算法能力、经验数据利用成为安全防护的关键要素

基于大数据精准分析

历史数据、机器学习、复杂数学模型等成为安全分析新宠

基于云提供安全服务

云的计算能力和光速使得本地网关被云网关替代成为现实

Thank you

www.huawei.com