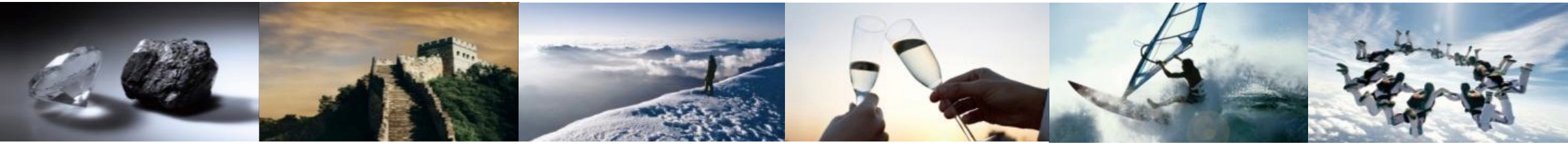
数梦工场
DtDream

NJSD 全球软件大会 2017

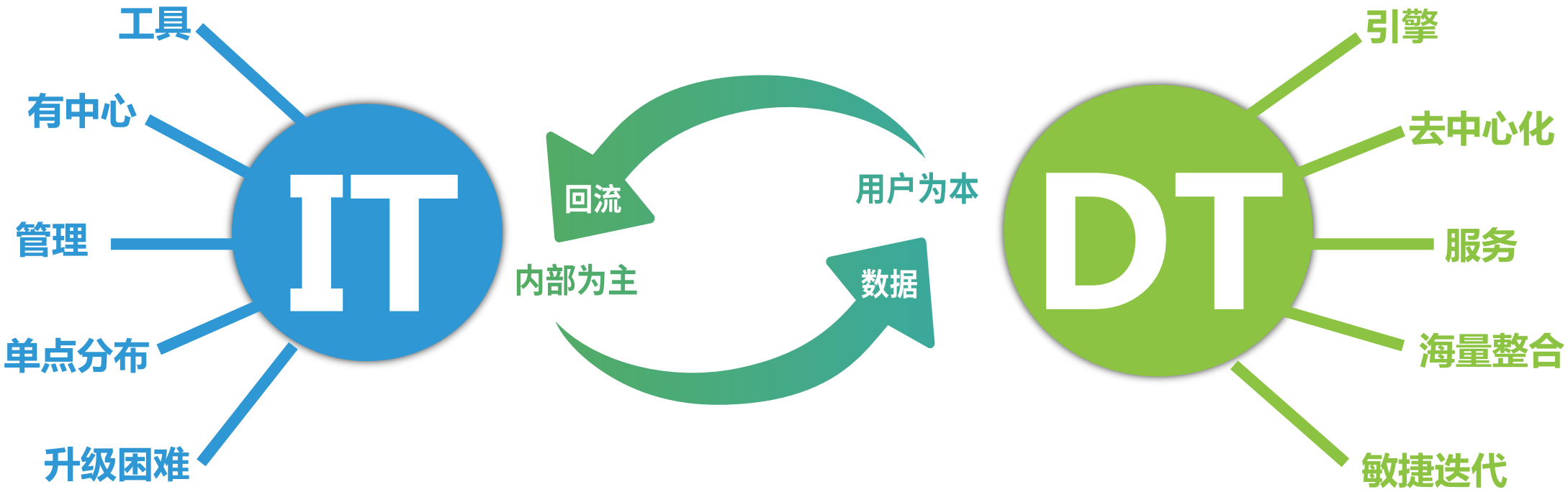
IT大咖说 知识分享平台

DT时代互联网安全防护的演进探讨



- 何为DT时代？
- IT时代互联网安全防护现状
- DT时代互联网安全防护探讨


阿里巴巴
Alibaba.com
DT
平台
数据
服务
Alibaba
DT生态
DT平台
Dt Dream
数梦工场
政府
公安
金融
企业


工具
有中心
管理
单点分布
升级困难
IT
回流
内部为主
用户为本
数据
DT
引擎
去中心化
服务
海量整合
敏捷迭代

DT时代—技术积累支撑下的思维质变

商业社会将以数据为核心和内在驱动力，推动社会发展的不再是对自然资源的利用（如石油、天然气等），而是以云计算、大数据为导向的技术革新，数据资源将会是众多利益集团必争的战略性资源之一，其将影响着农业、工业、第三产业的高层级变革。

云计算是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问， 进入可配置的计算资源共享池（资源包括网络，服务器，存储，应用软件，服务），这些资源能够被快速提供，只需投入很少的管理工作，或与服务供应商进行很少的交互。

——来自美国国家标准与技术研究院（NIST）的定义

云计算

云计算是一种资源集中后再进行按需分配、最优分配的理念，不光在计算、网络、存储等技术维度起到了极大的影响，其理念表达了整个社会各方面资源利用最优化配置的大趋势；

“大数据”是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力来适应海量、高增长率和多样化的信息资产

——来自Gartner的定义

大数据

当前大数据在很多应用场景第一步还是在于数据来源哪里、数据如何产生的阶段，数据的在线化、环流是首先要解决的问题；

DT时代，在强有力的技术、思维支撑下，很多以前想做但一直做不到的目标将成为现实。

- 何为DT时代？
- IT时代互联网安全防护现状
- DT时代互联网安全防护探讨

IT时代的安全防护

事前

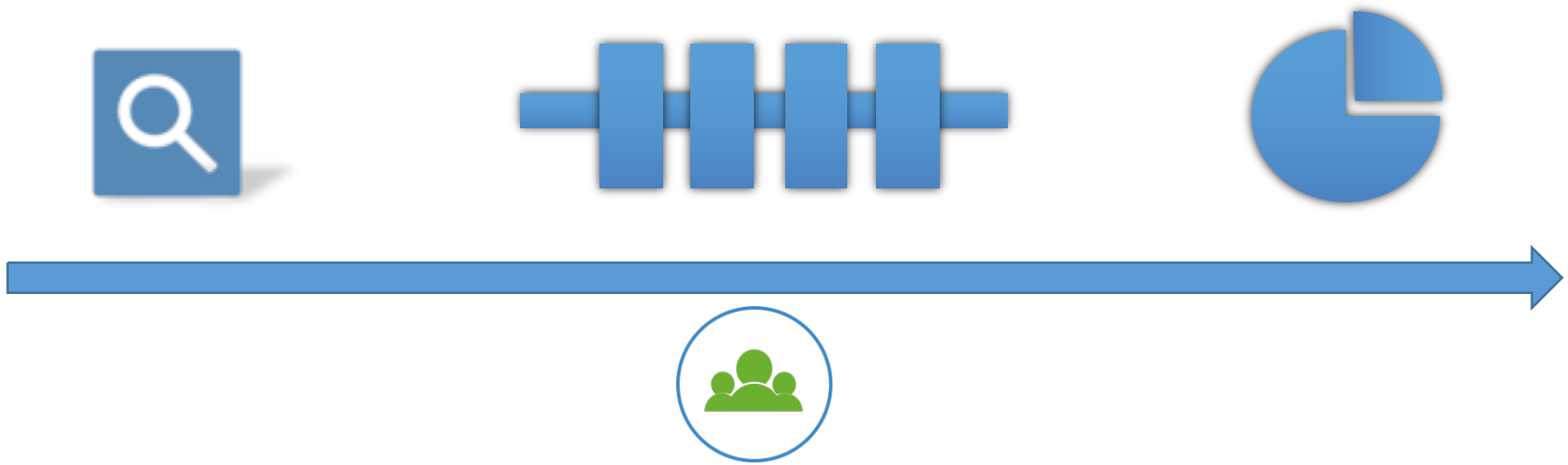
扫描渗透

事中

纵深防御

事后

安全报表



安全运维—本地驻场

IT时代的安全防护—事前

扫描渗透

滞后的漏洞扫描	程序化的渗透测试
CVE	Step1
MAPP	Step2
安全研究团队	Step3
…	…

IT时代的安全防护—事中

纵深防御

- DDoS防御 — 阈值检测
- 防火墙 — 规则匹配
- 入侵检测 — 特征匹配
- 入侵防御 — 特征匹配
- 网络防病毒 — 特征匹配
- Web防火墙 — 特征匹配

IT时代的安全防护—事后

安全报表


DDoS产品
控制台/报表


防火墙产品
控制台/报表


入侵检测产品
控制台/报表


入侵防御产品
控制台/报表


网络防病毒产品
控制台/报表

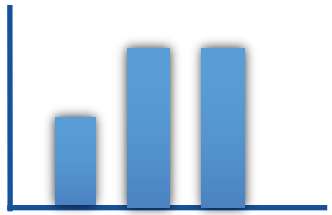

Web防火墙产品
控制台/报表

排名TOPN

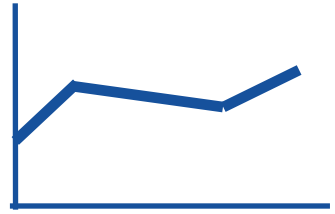
Top10 攻击者
Top10 被攻击资产
Top10 攻击方式

饼状图

柱状图



折线图



IT时代的安全防护—安全运维

安全服务

依赖本地驻场

防火墙策略配置

安全应急事件处理

漏洞修补

安全报告撰写

...

IT时代的安全防护

事前

“扫描渗透”

滞后的漏洞扫描

CVE

MAPP

安全研究团队

...

程序化的渗透测试

Setp1

Setp2

Setp3

...

传统漏洞扫描样本来源单一，不及时

渗透测试按部就班，程序化、效果不佳

事中

“纵深防御”

防火墙 IPS WAF 防病毒

现有防护体系：看似纵深实则割裂

当前检测能力：手段单一，误报、漏报高

事后

“安全报表”

排名TOPN 饼状图 柱状图 折线图

安全报表单独展现，无全局安全态势

数据展现以统计为主，实质意义不大

安全运维—本地驻场

严重依赖本地驻场 基础工作为主 救火是主旋律

IT时代的安全防护

检测/防护手段相对不变

用户孤独的面对攻击威胁

基本只能被动挨打

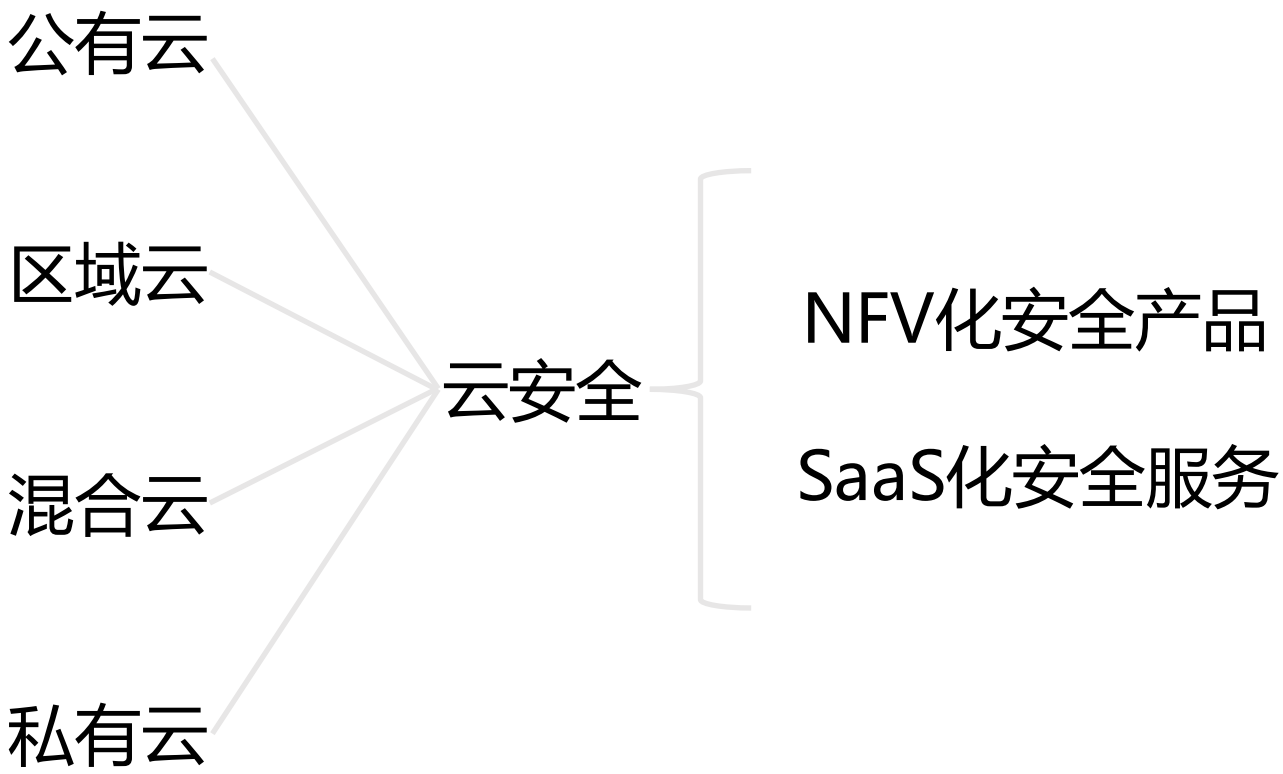
- 何为DT时代？
- IT时代互联网安全防护现状
- DT时代互联网安全防护探讨

DT时代，安全防护也正在变化，并且安全技术、理念的变化脱离不开大的技术环境影响。

DT时代的安全演进驱动力

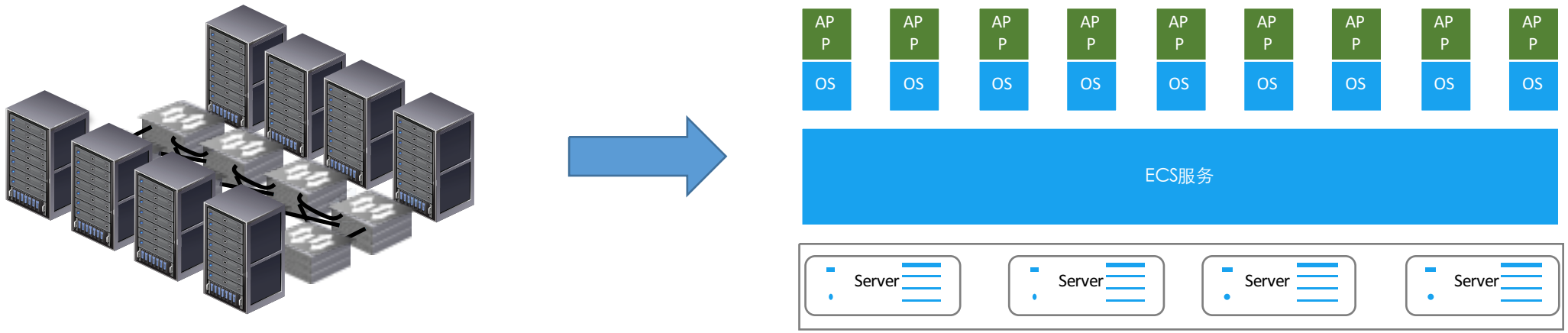
云计算　　大数据　　安全思考

云计算对安全影响—云场景交付形态



主要解决安全能力场景化部署适应性的问题

云计算对安全影响—防护对象的在线化



资产台账的问题解决对绝大多数用户安全工作有极大的现实意义

云计算对安全影响—事前弱点发现

滞后的漏洞扫描

CVE

MAPP

安全研究团队

...

在线化的弱点扫描
- 云端扫描
- 与云端相连的扫描

应急0day情报服务
- 与云端相连的扫描

云计算对安全影响—事前红蓝对抗

白帽子资源池化 → 多样的渗透手段 → 按效果付费的商业模式

渗透测试工程师 → 固化的渗透手段 → 按次付费的商业模式

云计算对安全影响—安全运维

云端安全专家运维

本地驻场安全运维

- 解决全国范围内安全人员匮乏问题
- 提升对用户服务的安全人员水平
- 反向提供安全人员的问题处理经验
- 共享安全策略配置与事件防护处理经验

大数据对安全影响

对大多数用户与传统安全厂商而言：
安全大数据也是如此

IT时代的安全数据分析

SIEM（安全事件和信息管理）/SOC（安全运行中心）

—业界对安全数据分析的原始尝试

应用目标	**安全设备众多需实现统一监管**	**看清安全，及时进行安全事件发现及追溯**	**解决安全问题，形成安全工作闭环**
落地效果	□□基本实现	□□难以实现	□□基本实现

IT时代的安全数据分析—数据来源

这样的数据来源决定了SIEM/SOC无法获取到在攻防方面的最真实数据

UNIX操作系统

- IBM AIX
- Sun Solaris
- HP-UX
- SuSe Linux
- RedHat Enterprise Linux
- SCO Unix
- Free BSD

WINDOWS操作系统

- Windows NT/2000/XP/2003/7/8

异常流量监控设备

- Arbor PeakFlow

防火墙

- Cisco ASA
- Cisco Pix
- Checkpoint
- Fortigate
- NetEye
- NetPower
- Nokia
- Juniper NetScreen
- LinkTrust Cyberwall
- Microsoft ISA Firewall
- SonicWall
- WatchGuard 8000

网络设备

- Cisco路由器、交换机
- Juniper路由器、交换机
- 华为路由器、交换机
- Extreme交换机
- Radware AppDirector 202

IDS

- LinkTrust IDS
- LinkTrust IPS
- NetPower
- TippintPoint IPS
- 绿盟冰之眼IDS
- ISS realsecure
- Radware
- Gnu Snort
- 天融信IDS
- 华为IPS
- 华为3C IPS
- 启明IDS

终端管理

- Linktrust Intrasec
- 北信源
- LanDesk
- 圣博润

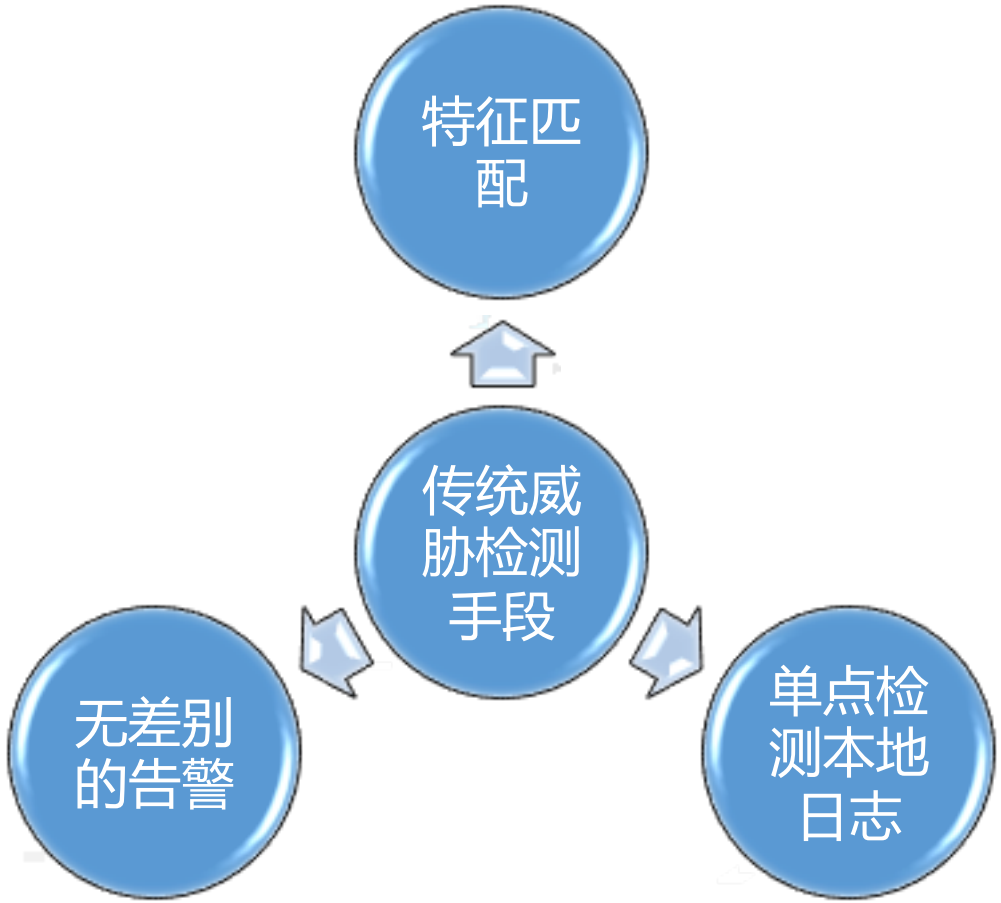
安全访问网关

- Symark
- LinkTrust Unix访问控制网关
- 华为网关
- 亚信网关
- 东信网关
- 天融信网关
- 联想网御网关
- 网御神州
- 启明星辰网关

防病毒

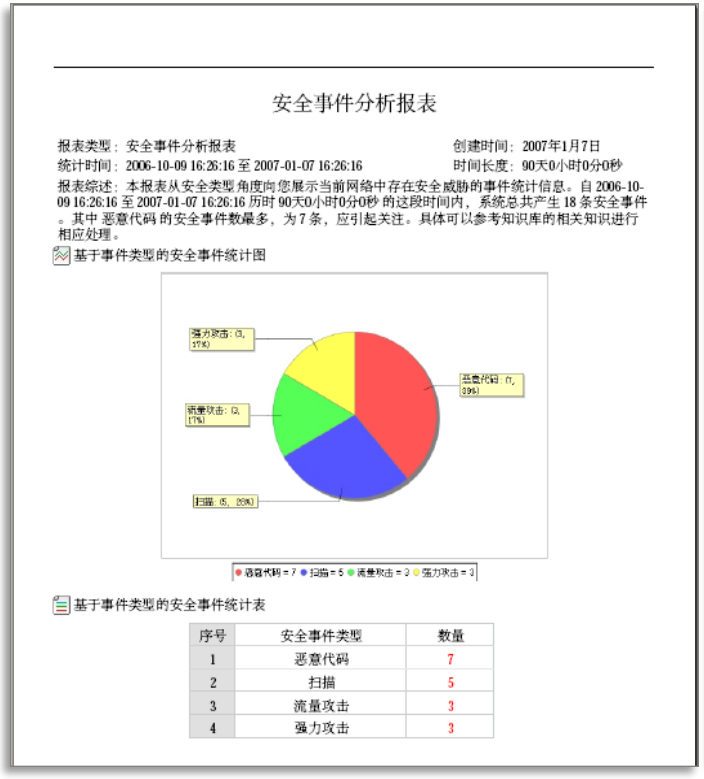
- TrendMicro TMCM
- TrendMicro NVW
- Symantec 8/9/10/11
- 瑞星

IT时代的安全数据分析—数据来源



IT时代的安全数据分析—利用数据的思路

在数据的分析、利用上SOC秉承了传统安全的那套思路，主要以统计、排名为主



安全事件分析报表

报表类型：安全事件分析报表　　创建时间：2007年1月7日

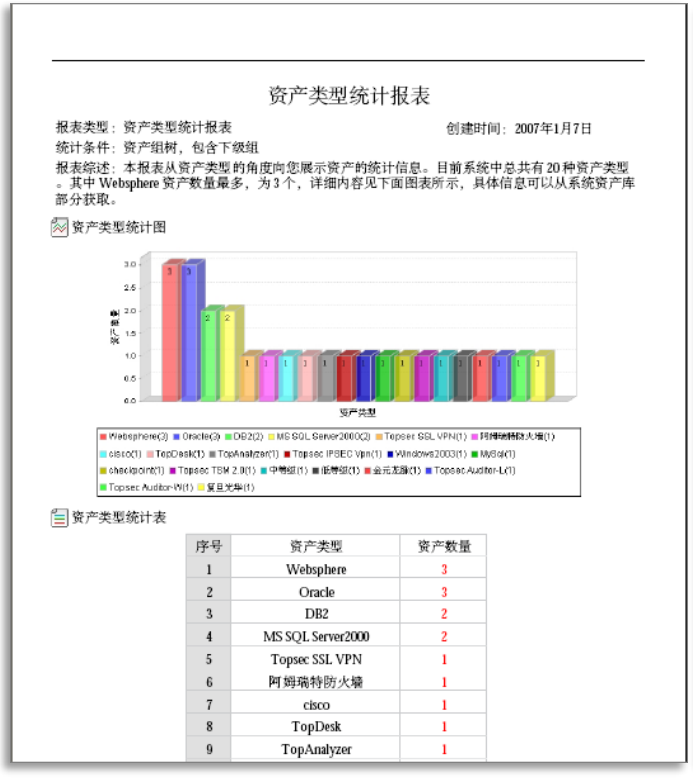
统计时间：2006-10-09 16:26:16 至 2007-01-07 16:26:16　　时间长度：90天0小时0分0秒

报表综述：本报表从安全类型角度向您展示当前网络中存在安全威胁的事件统计信息。自 2006-10-09 16:26:16 至 2007-01-07 16:26:16 历时 90天0小时0分0秒 的这段时间内，系统总共产生 18 条安全事件。其中 恶意代码 的安全事件数最多，为 7 条，应引起关注。具体可以参考知识库的相关知识进行相应处理。

基于事件类型的安全事件统计图

基于事件类型的安全事件统计表

序号	安全事件类型	数量
1	恶意代码	7
2	扫描	5
3	流量攻击	3
4	强力攻击	3



资产类型统计报表

报表类型：资产类型统计报表　　创建时间：2007年1月7日

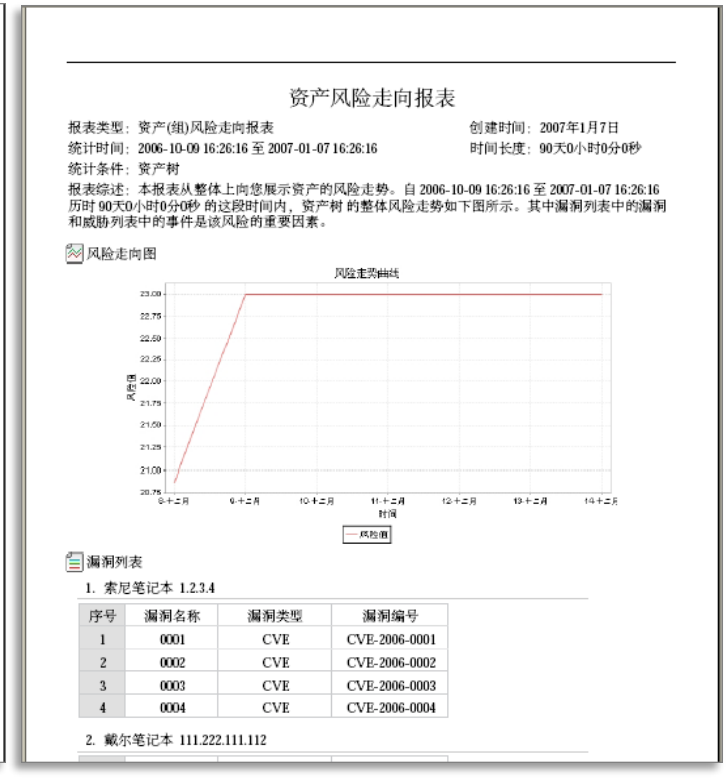
统计条件：资产组树，包含下级组

报表综述：本报表从资产类型的角度向您展示资产的统计信息。目前系统中总共有 20 种资产类型。其中 Websphere 资产数量最多，为 3 个，详细内容见下面图表所示，具体信息可以从系统资产库部分获取。

资产类型统计图

资产类型统计表

序号	资产类型	资产数量
1	Websphere	3
2	Oracle	3
3	DB2	2
4	MS SQL Server2000	2
5	Topsec SSL VPN	1
6	阿姆瑞特防火墙	1
7	cisco	1
8	TopDesk	1
9	TopAnalyzer	1



资产风险走向报表

报表类型：资产(组)风险走向报表　　创建时间：2007年1月7日

统计时间：2006-10-09 16:26:16 至 2007-01-07 16:26:16　　时间长度：90天0小时0分0秒

统计条件：资产树

报表综述：本报表从整体上向您展示资产的风险走势。自 2006-10-09 16:26:16 至 2007-01-07 16:26:16 历时 90天0小时0分0秒 的这段时间内，资产树 的整体风险走势如下图所示。其中漏洞列表中的漏洞和威胁列表中的事件是该风险的重要因素。

风险走向图

漏洞列表

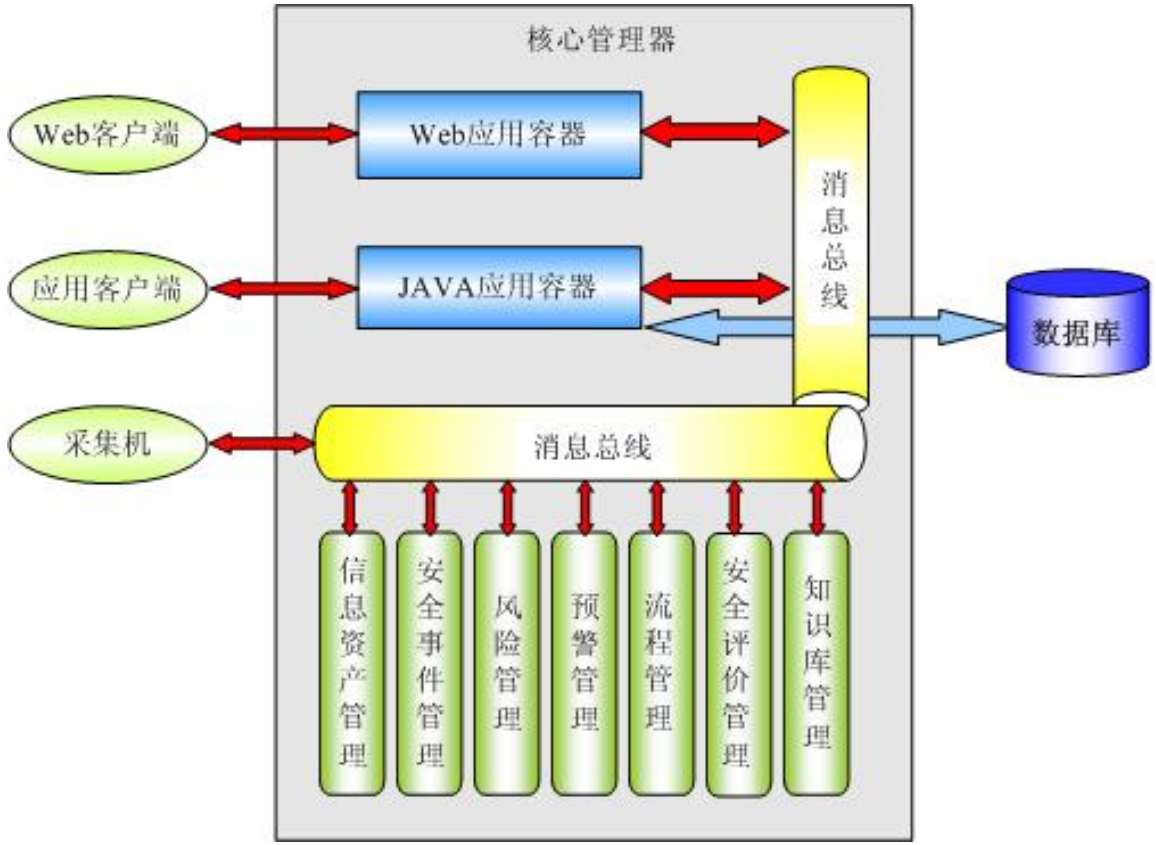
1. 索尼笔记本 1.2.3.4

序号	漏洞名称	漏洞类型	漏洞编号
1	0001	CVE	CVE-2006-0001
2	0002	CVE	CVE-2006-0002
3	0003	CVE	CVE-2006-0003
4	0004	CVE	CVE-2006-0004

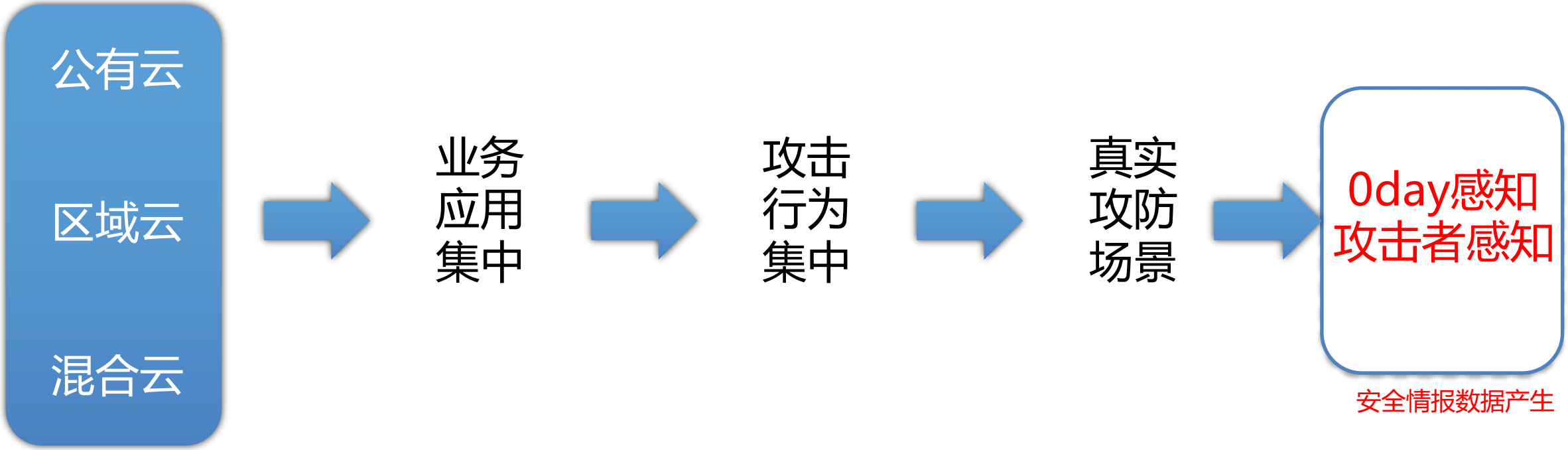
2. 戴尔笔记本 111.222.111.112

IT时代的安全数据分析—平台架构的局限

传统的简单数据库承载架构不足以支撑大数量下的复杂的分析事项

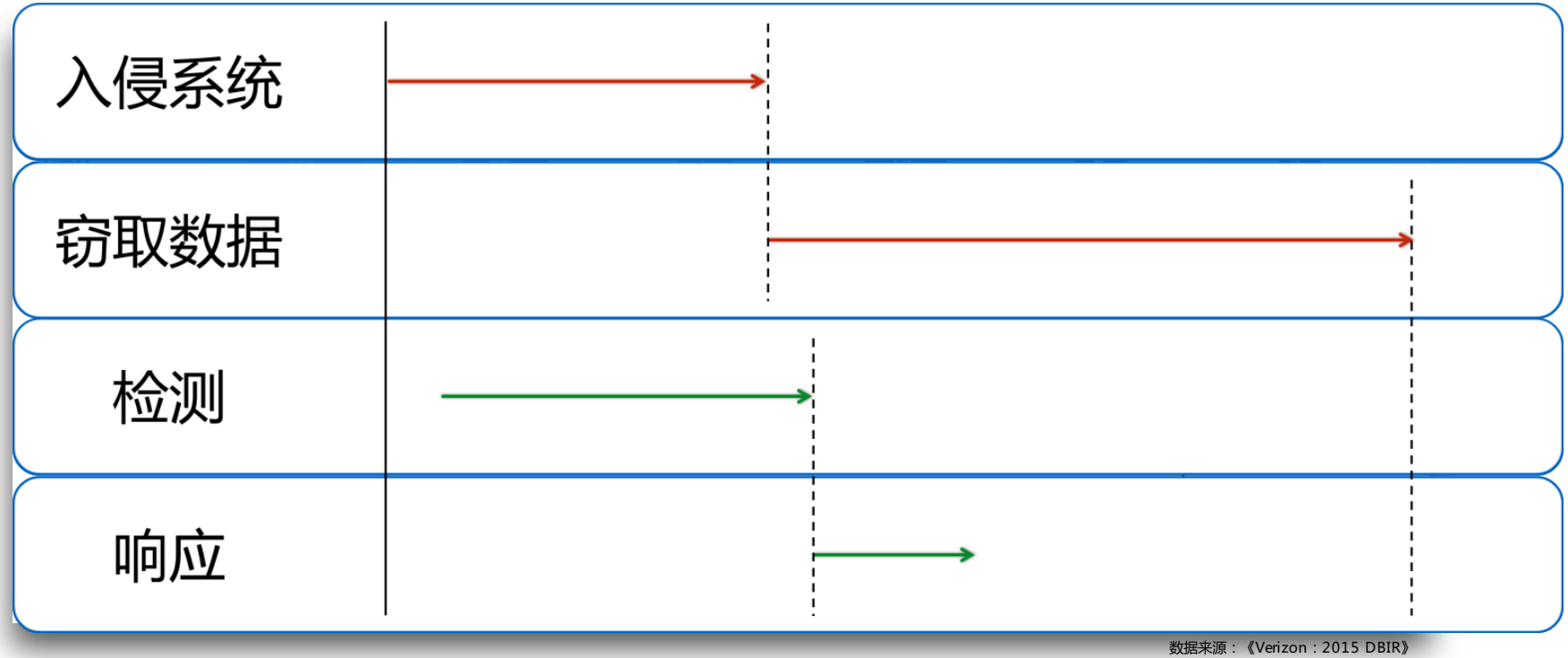


云计算带来了第一份安全大数据



云计算安全服务提供商正在获得最为宝贵的安全防护数据

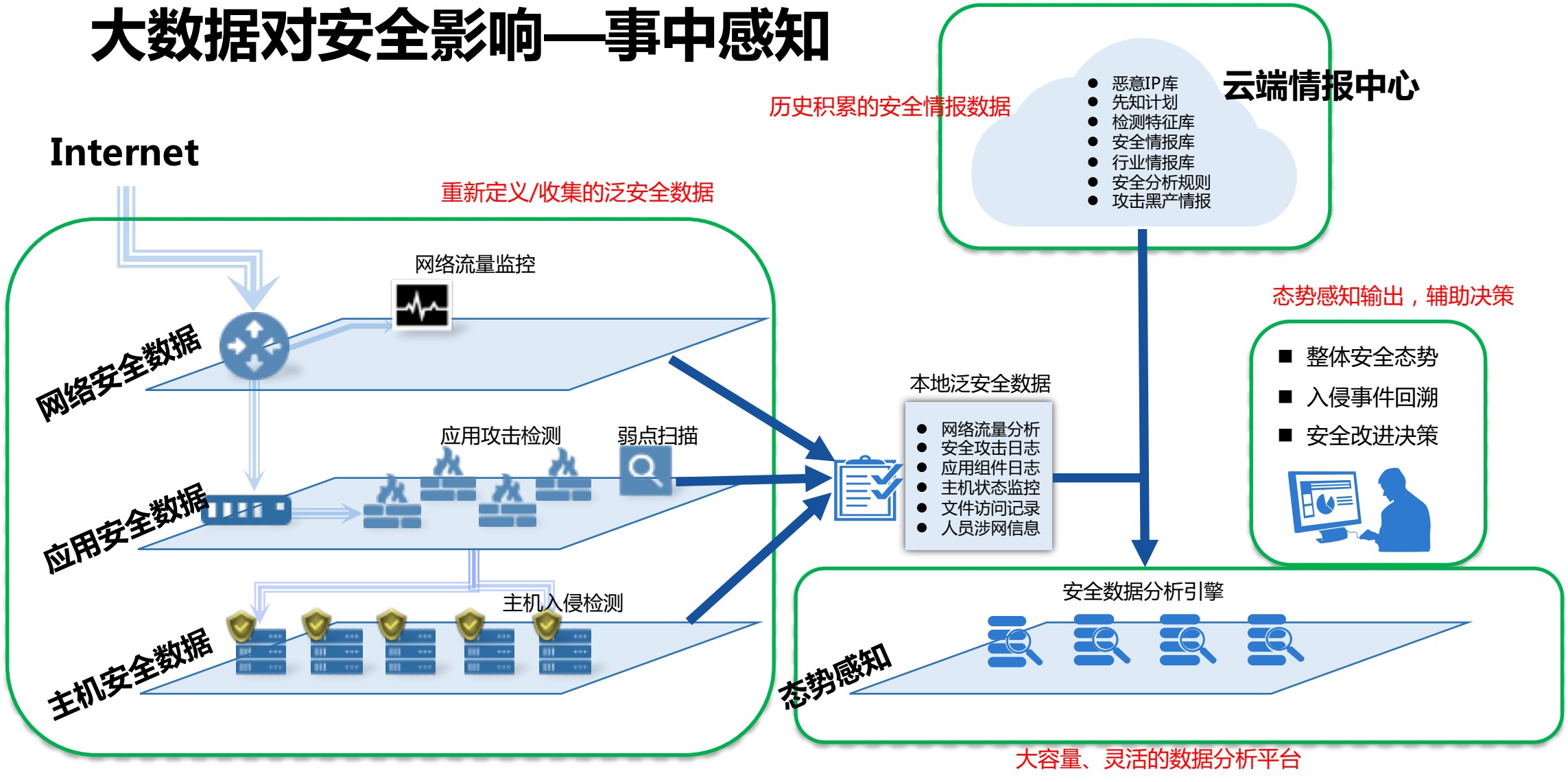
大数据对安全影响—事中感知



数据来源：《Verizon：2015 DBIR》

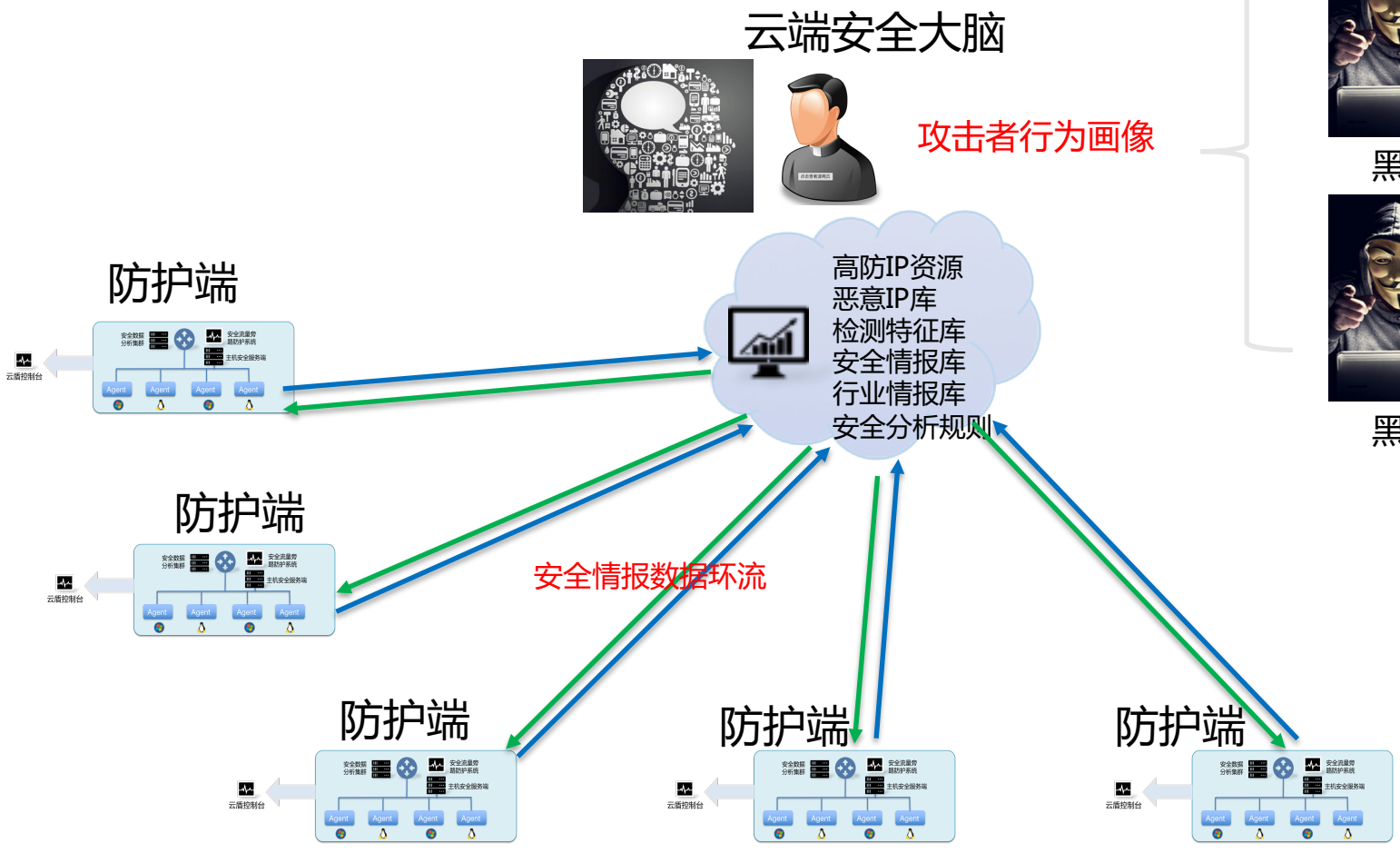
增加敌人入侵系统和窃取数据的耗时	纵深防御	Protect
提高自己检测入侵及数据泄露的能力和速度	态势感知	Detect
提高自己应急响应的速度和能力	威胁联动 安全运营	React

大数据对安全影响—事中感知



大数据对安全影响—事中感知

大数据对安全影响—事中感知




黑客A

黑客B

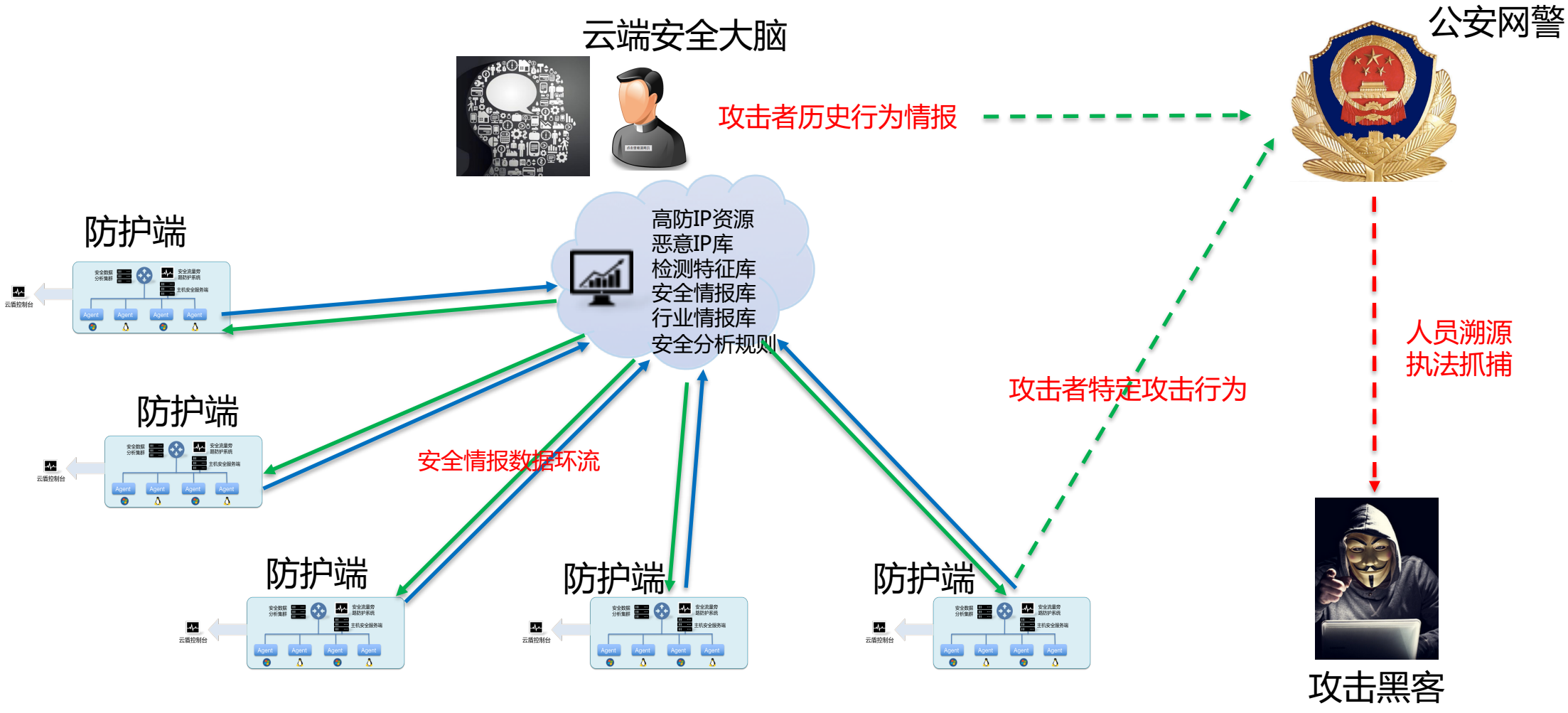

黑客C


黑客D

- 攻击行业分布
- 攻击手段组成
- 攻击行为习惯
- 攻击成功样例
- 攻击水平评价
- 攻击趋势预测

…

大数据对安全影响—事后反击



DT时代的安全防护—全面提升

事前	事中	事后
白帽众测 漏洞情报	纵深防御 攻防态势	反击黑客

安全运维—云端专家

DT时代的安全防护

感知与防御联系，动态防御　攻击者信息共享，共同抵御　主动追溯，威慑攻击者


用最卓越的数据技术，
去实现
最美好的人类梦想。
数梦工场

数梦工场

DtDream