WOTA

51CTO

World Of Tech 2017

# 全球架构与运维技术峰会

2017年4月14日-15日　北京富力万丽酒店

ARCHITECTURE

WOTA

51CTO

出品人及主持人：

# 于　雪

51CTO WOT大会主编

# 主动安全防御体系构建

# 构建面向威胁的企业网络安全防御体系

徐洪涛

Cisco

WOTA

51CTO

# 徐洪涛

思科

大中华区安全业务技术总监

分享主题：

## 构建面向威胁的企业网络安全防御体系

# 议题

- 2016年网络安全分析
  - 《思科2017年度安全报告解读》
- 构建面向威胁的网络安全防御体系

# 数据来源：思科遥感勘测与调查

全球

2017 年安全能力基准研究

- 每天 160 亿个网络请求
- 每天 6000 亿封电子邮件
- 总体而言，每天拦截近 200 亿个威胁
  - 每天超过 150 万个独特恶意软件样本
- 185 亿次 AMP 查询

CloudLock 遥感勘测

- 管理 1000 万名用户
- 跟踪 150 亿名用户的活动
- 发现 222,000 个应用
- 每天监控 10 亿个文件

时间贯穿2016 年的整个夏季

研究包括 13 个国家/地区

| | |
|---|---|
| 美国 | 中国 |
| 巴西 | 印度 |
| 德国 | 日本 |
| 意大利 | 墨西哥 |
| 英国 | 俄罗斯 |
| 澳大利亚 | 法国 |
| | 加拿大 |

受访者超过 2900 名

| | |
|---|---|
| 首席安全官 | 49% |
| 安全运营经理 | 51% |
| 超大型企业 | 12% |
| 大型企业 | 38% |
| 中型企业 | 50% |

# 与日俱增的数据流量导致受攻击面不断扩大

到 2020 年，全球 IP 流量将增长三倍

2.3

ZB

全球每年 IP 流量

66%

66% 的 IP 流量将源于 Wi-Fi 和移动设备

82%

82% 的消费者互联网流量将源于互联设备

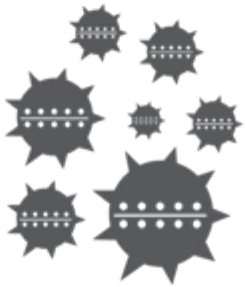
2x

宽带速度

# 攻击过程：行动时间越来越长

侦测

研究、确定和选择目标



制作武器

搭配使用远程访问恶意软件和漏洞攻击包

运送武器

通过邮件、网站和附件运送网络武器

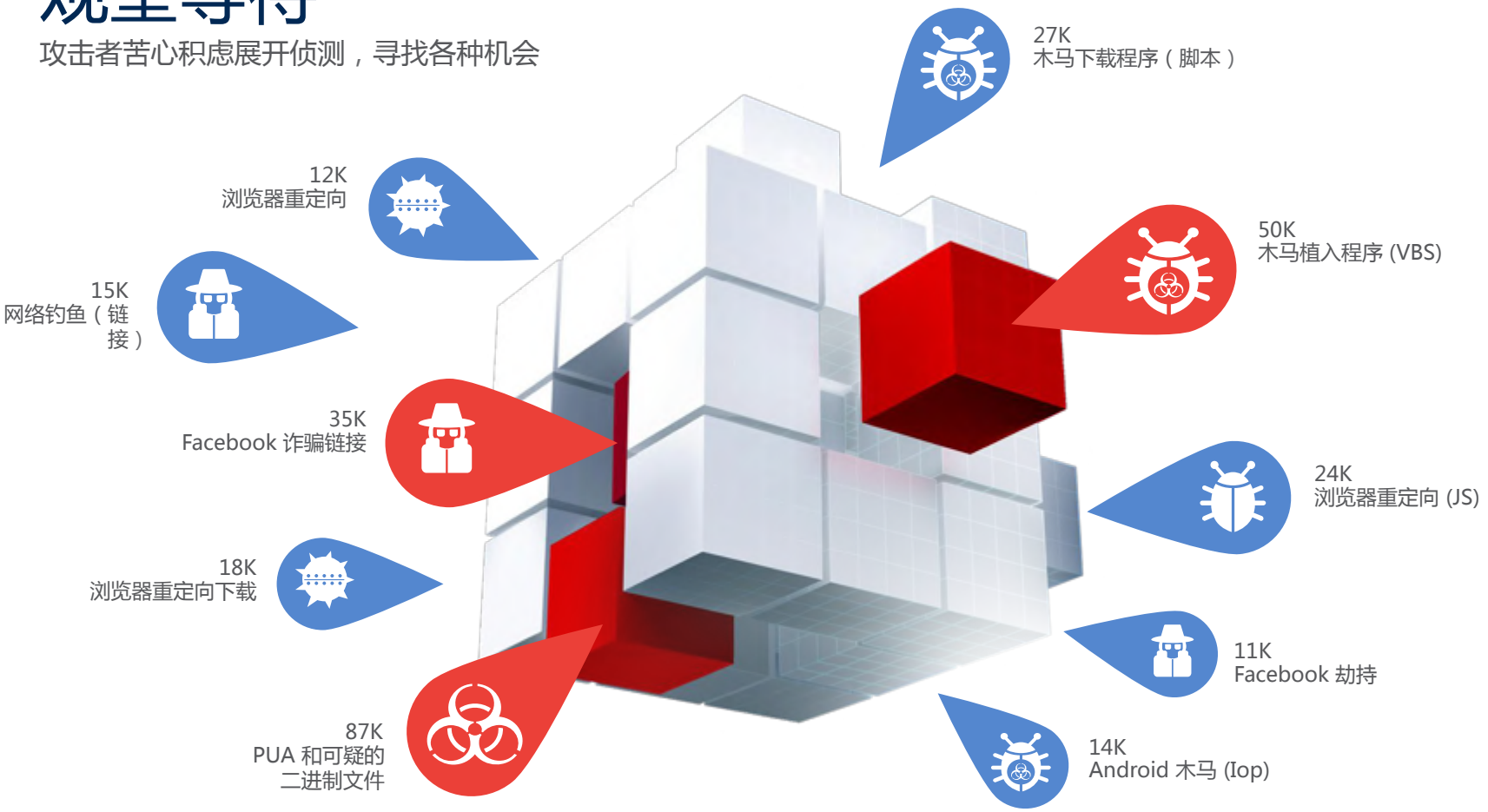
安装

安装负载，获得永久访问权限

侦测

# 观望等待

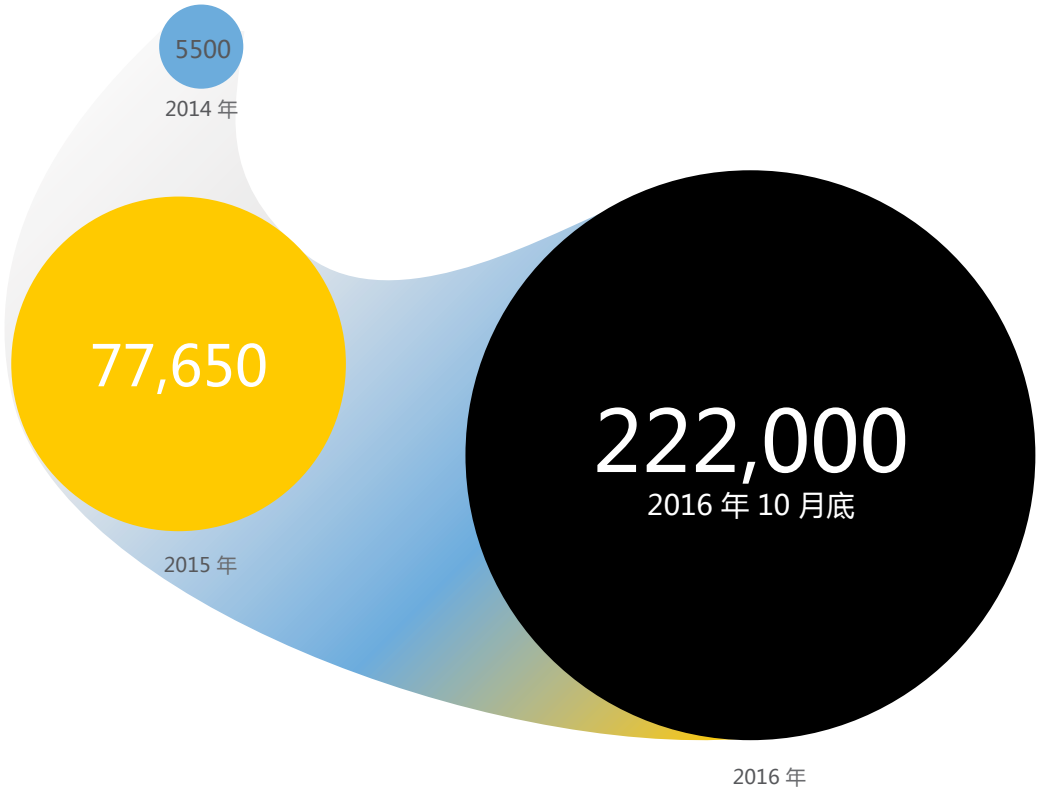
攻击者苦心积虑展开侦测，寻找各种机会

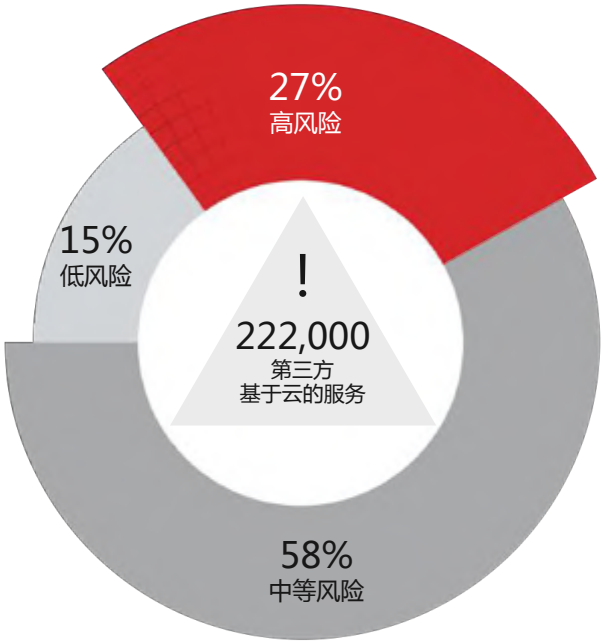


制作武器

# 基于云的服务急剧增长

互联的第三方基于云的服务导致安全边界迅速消散




基于 CloudLock 的云应用风险指数风险因素

运送武器

# 广告软件和恶意广告高速肆虐

## 恶意广告

利用代理（网关）提高速度和敏捷性

无需更改重定向，即可在服务器之间快速切换

ShadowGate：一种具成本效益的攻击活动

## 广告软件

**75%**

75% 的受访组织受到广告软件感染

运送武器

# 垃圾邮件卷土重来

邮件再度风行


65%

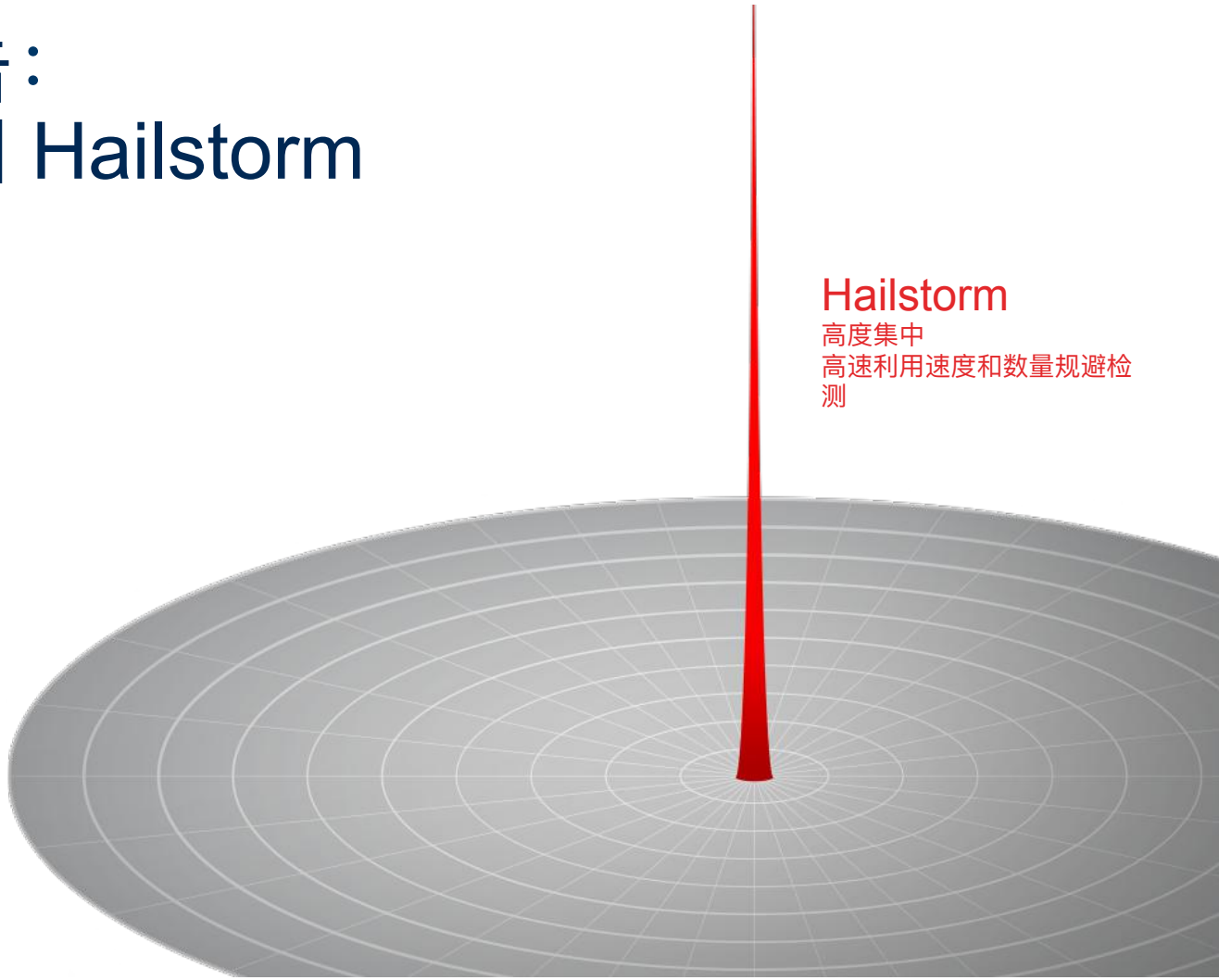
65% 的邮件是垃圾邮件

8%

8% 的垃圾邮件是恶意邮件

运送武器

# 垃圾邮件攻击：Snowshoe 和 Hailstorm



## Hailstorm

高度集中
高速利用速度和数量规避检测

## Snowshoe

利用不同的 IP 地址
通过少量发送邮件规避检测

运送武器

# 漏洞日益增多

攻击者在服务器端寻找行动空间和时间中间件容易招致攻击者的攻击

服务器
(从 2332 到 3142)

▲ 34%

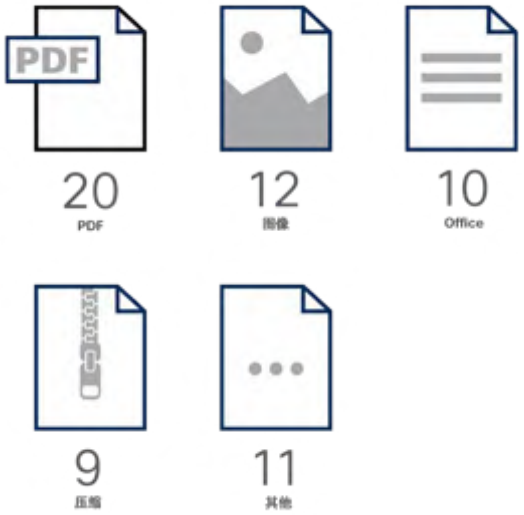
客户端
(从 2300 到 2106)

▼ 8%

网络
(从 501 到 396)

▼ 20%

中间件漏洞



安装

# Web 攻击方法：长尾效应

**具有危险性，但可以轻松避免和修复**


cisco

# TTE: 演进时间

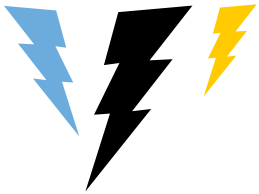
恶意软件系列行为恶劣；消除攻击者试图利用的机会

**文件类型**

攻击者通过各种文件类型（例如 .zip、.exe、.js、.docm、.wsf）轮番发起攻击

**传送机制**

攻击者通过网络和邮件实施部署



**演进速度**

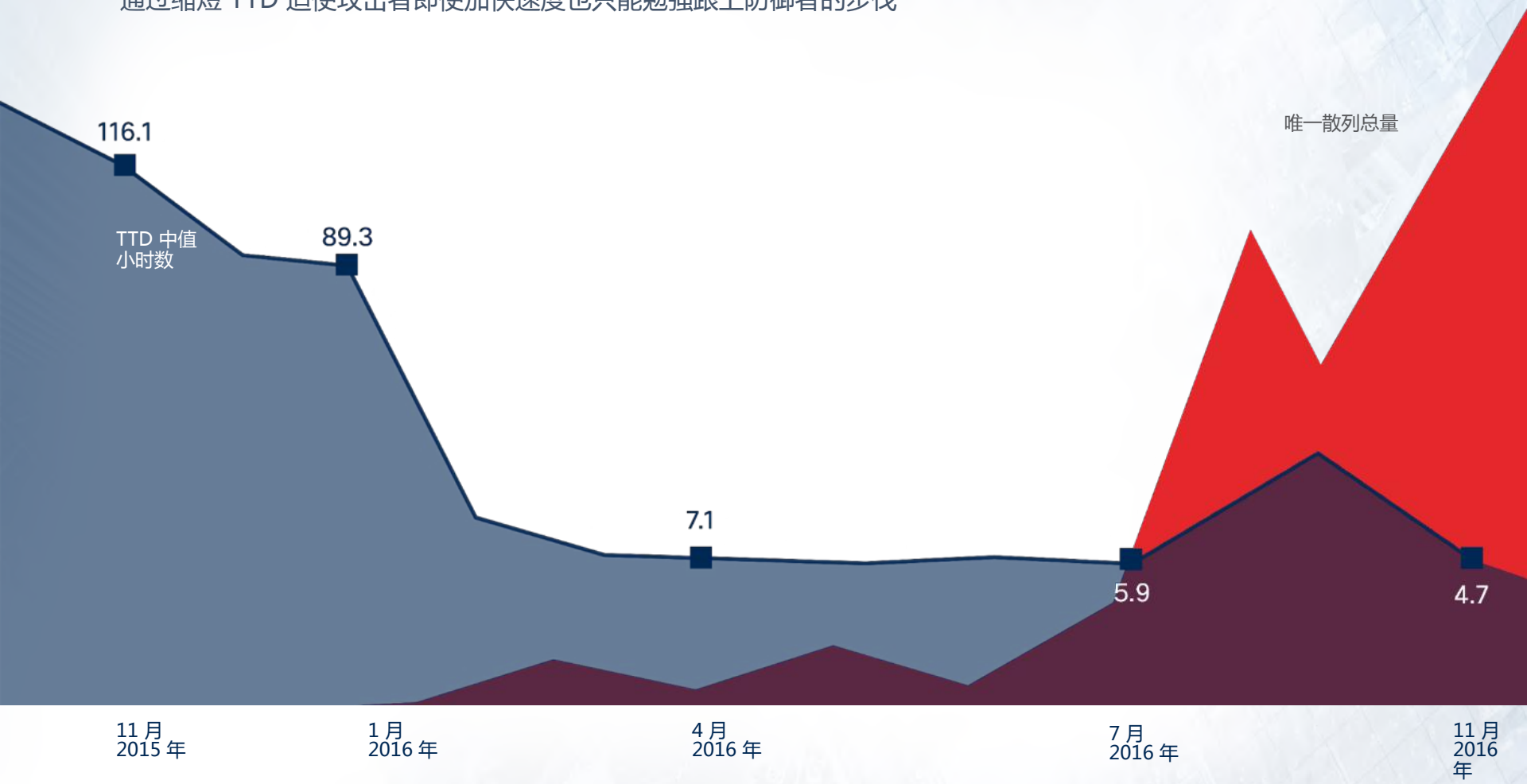
当旧文件的攻击效力开始下降时，攻击者会迅速演进并生成新的文件

**TTD（平均检测时间中值）**

防御者需要缩短 TTD，击溃攻击者

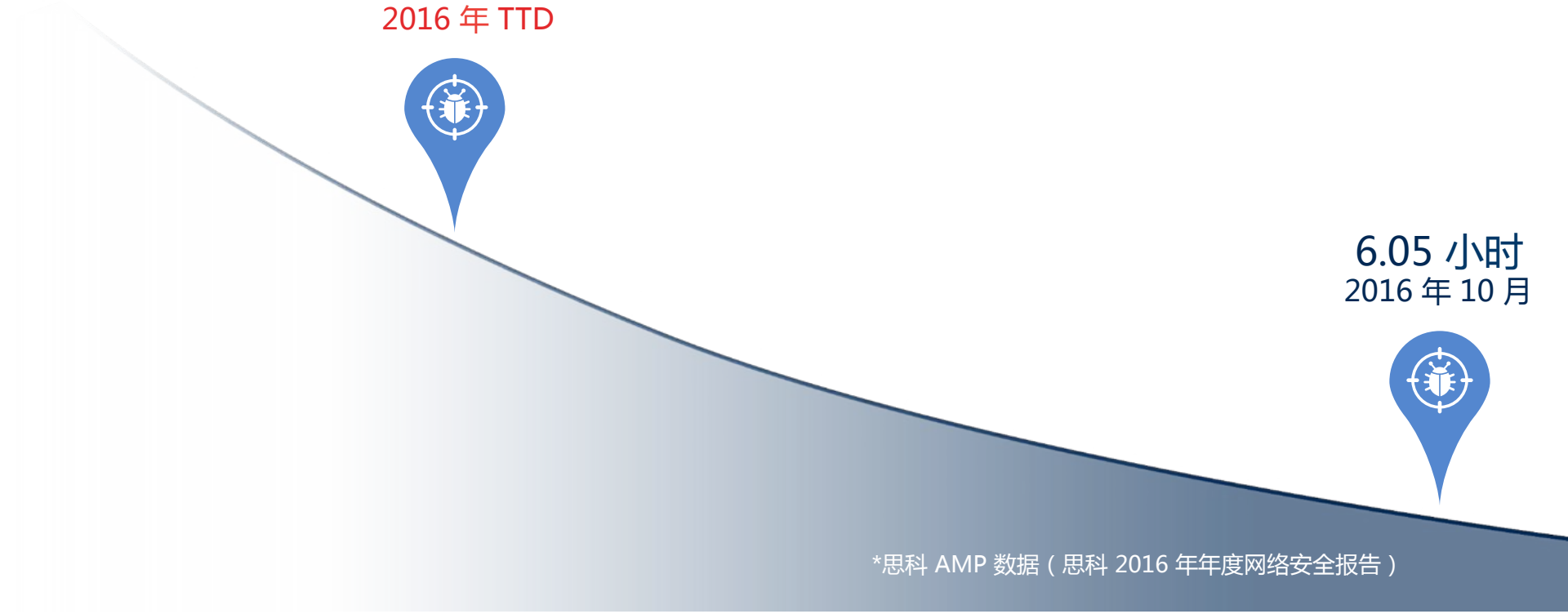
# TTE：唯一散列与 TTD (Locky)

通过缩短 TTD 迫使攻击者即使加快速度也只能勉强跟上防御者的步伐



# 思科安全事务高层管理者长期致力于缩短 TTD

从 2016 年 5 月至 10 月，TTD 缩短了 9.14 小时




*思科 AMP 数据（思科 2016 年年度网络安全报告）

CISCO

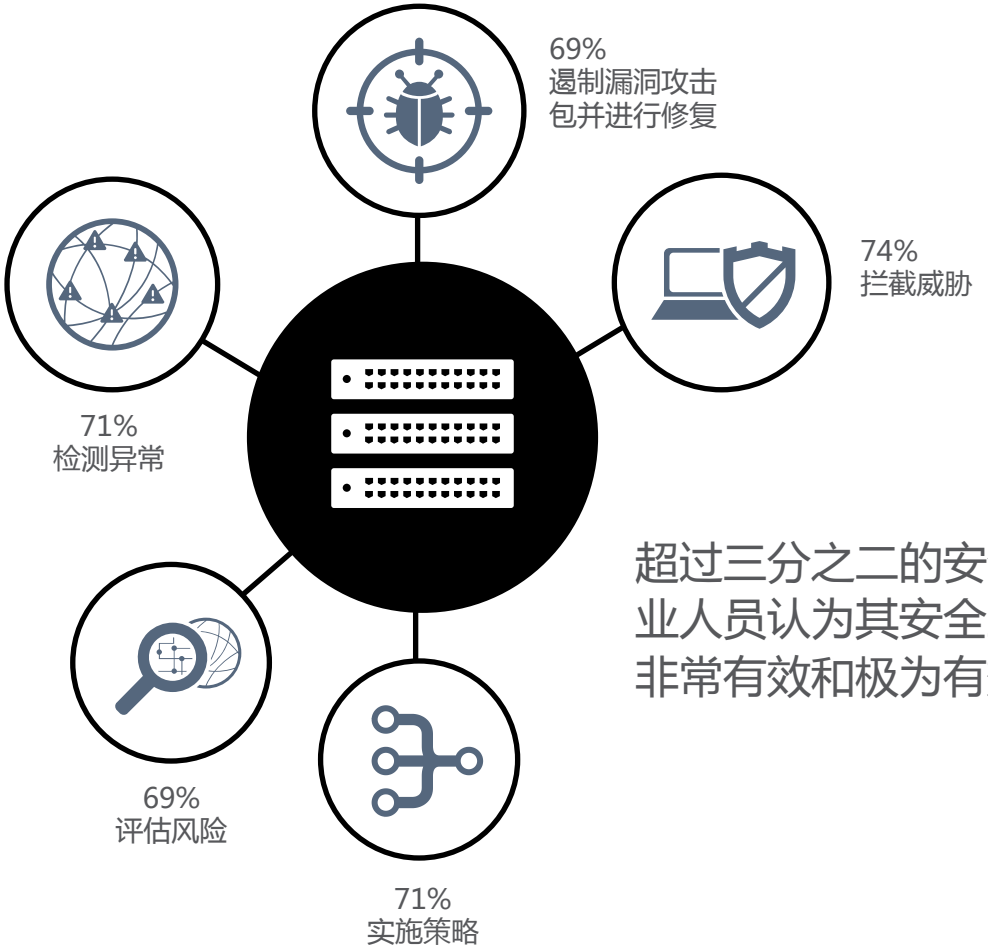
# 日益紧张的保护时间

## 您的表现必须达到何种水平才算优秀？

# 感知 高效工具

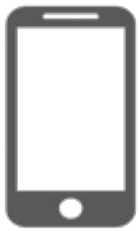
58%

58% 的安全专业人员认为其安全基础设施达到了最新水平。




超过三分之二的安全专业人员认为其安全工具非常有效和极为有效。

# 安全专业人员认为在防御网络攻击方面存在 4 个主要关注领域



移动设备

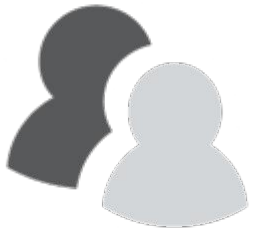
58%

公共云中的数据

57%

云基础设施

57%



用户行为

57%

百分比表示认为界定相应类别非常困难和极为困难的受访者比例

# 提高安全性面临的最大障碍

## 企业限制

35%
预算
(-4%)

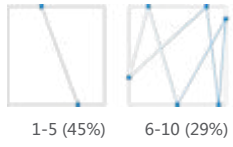
28%
兼容性问题
(-4%)

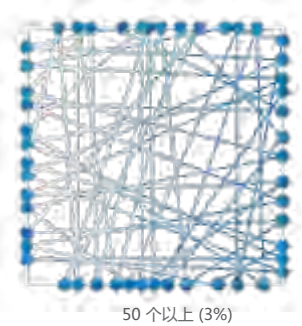
25%
缺少经过培训的人员
(+3%)

25%
认证要求
(+/-0%)

（相对 2015 年的变化）

## 复杂性



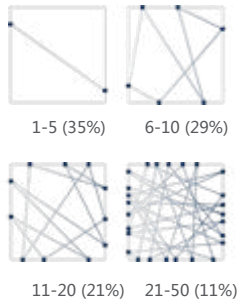



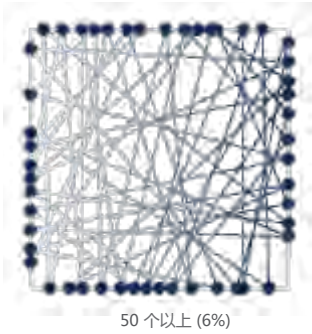

供应商

55%

55% 的组织使用 6 至 50 个以上安全供应商

2016 年 (n=2,850)




产品

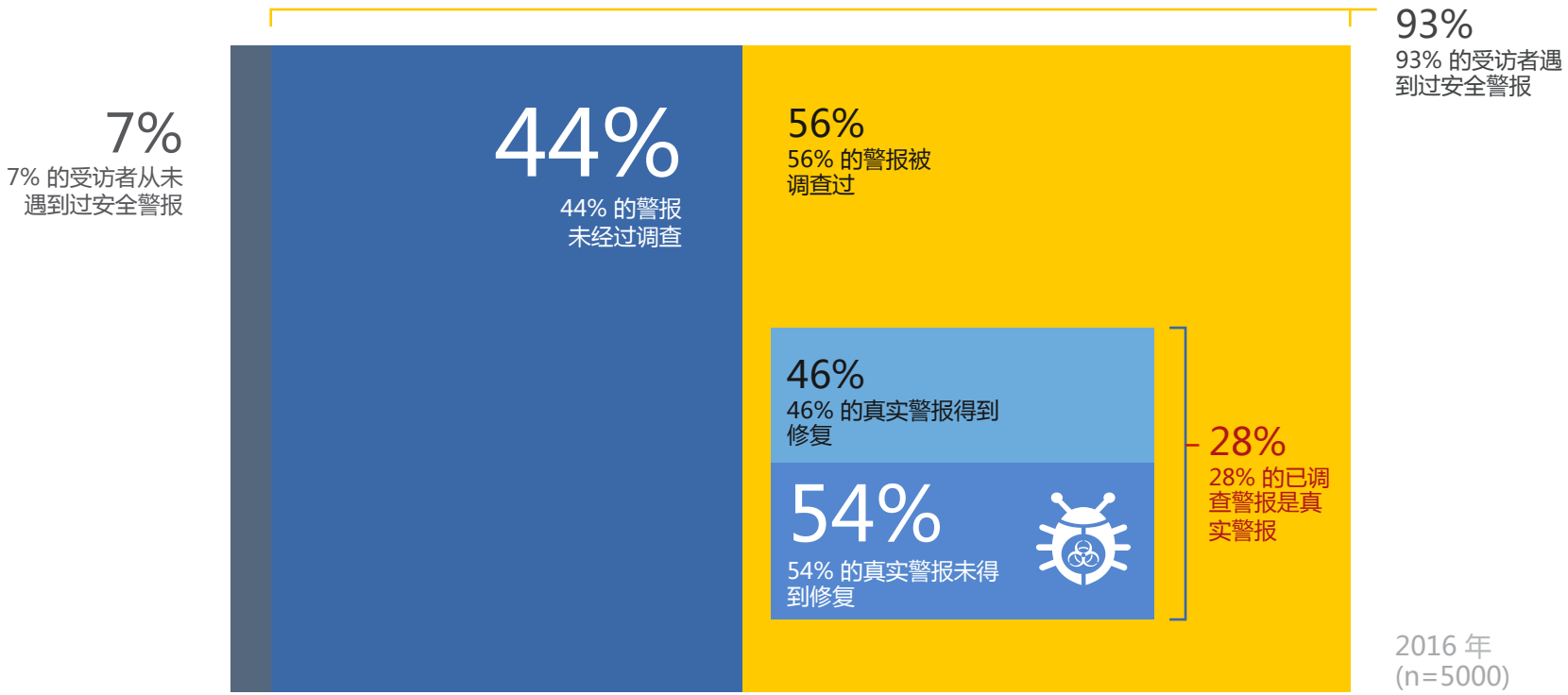
65%

65% 的组织使用 6 至 50 个以上安全产品

2016 年 (n=2,860)

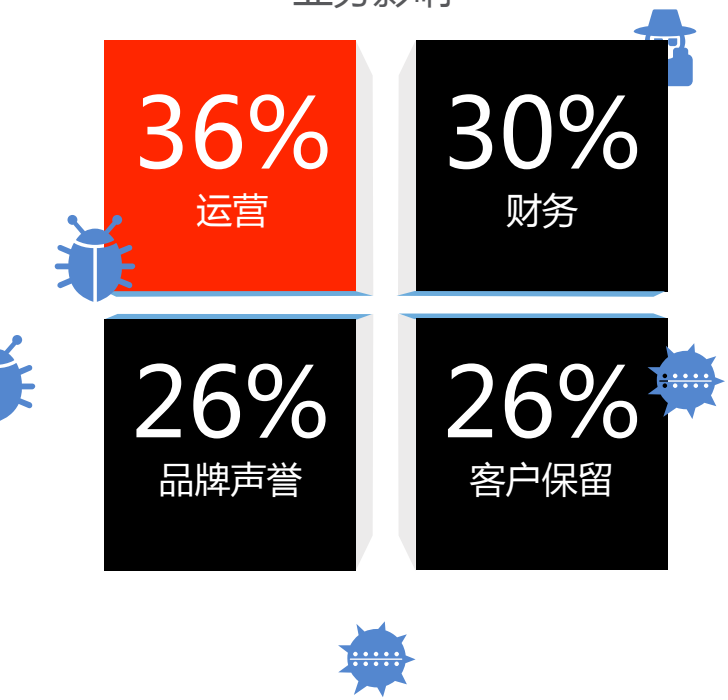
# 超过 40% 的安全警报从未经过调查：为什么？

未调查的警报导致巨大的业务风险



# 沉重打击：安全事件导致系统瘫痪并对重要业务运营造成不良影响

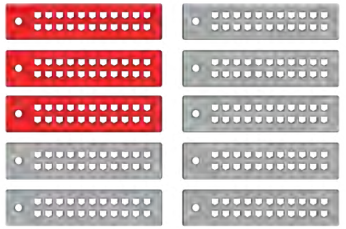
业务影响




运营影响

**1-8 小时**

65% 的组织遭遇 1-8 小时的系统停机



**近 30%**

61% 的组织中有近 30% 的系统受到影响

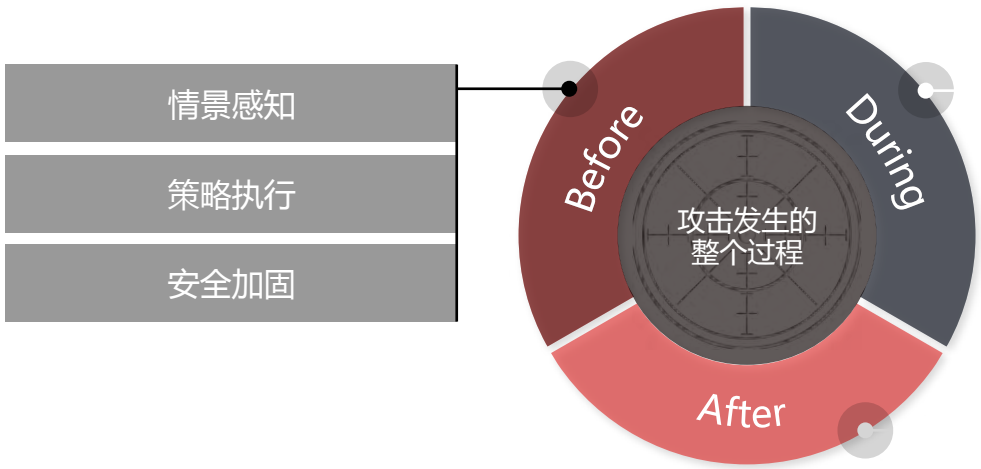
# 议题

- 2016年网络安全分析
  - 《思科2017年度安全报告解读》

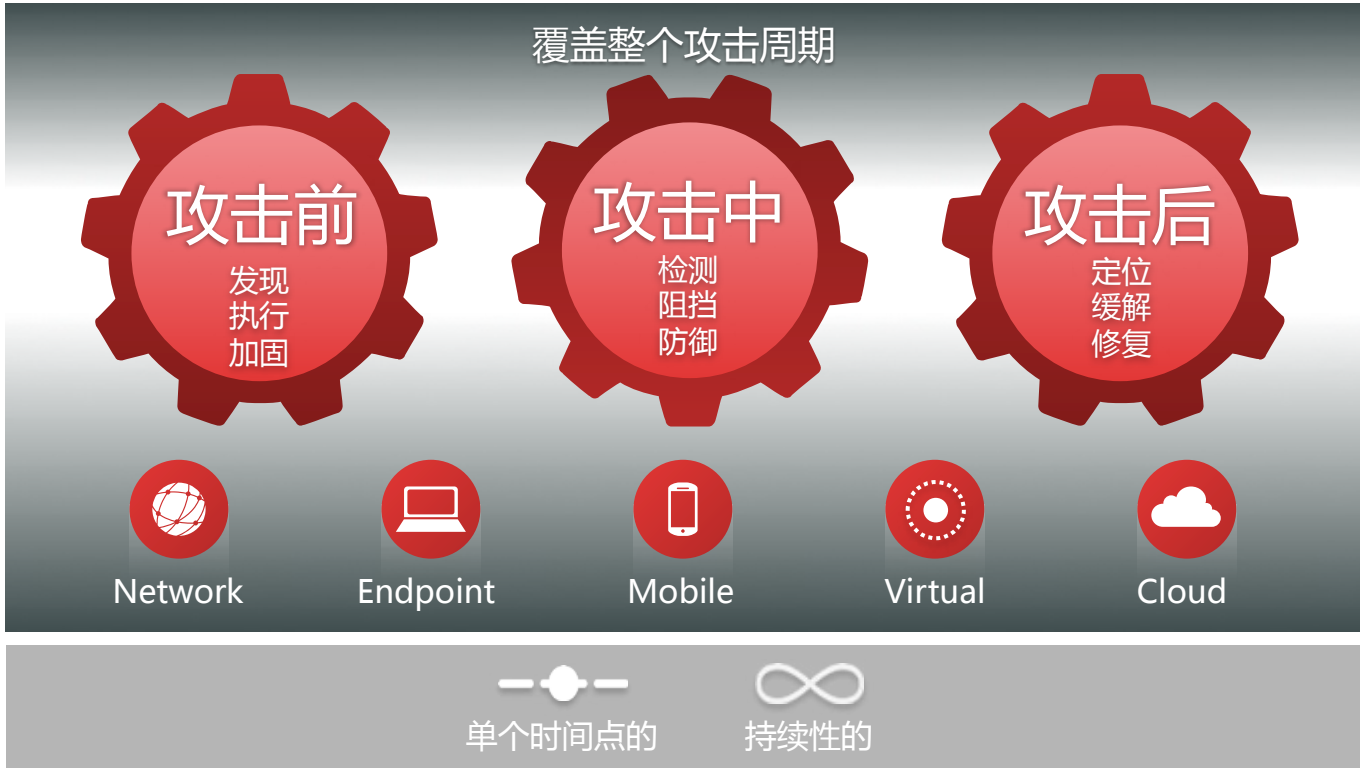
- 构建面向威胁的网络安全防御体系

# 我们该如何防御？

## 从攻击者的视角考虑安全防御问题



# 我们需要涵盖整个攻击周期的动态防御体系



# 构建基于威胁的防御平台的关键点

## 提高可见性 Visibility-Driven

与网络设备集成，
情景感知
自动化
提供安全防护的准确依据

## 关注威胁 Threat-Focused

高级威胁防御
云安全智能
减少恶意威胁造成的损失

## 统一平台 Platform-Based

灵活开放平台，
可扩展，全面控制与管理
提供统一动态的安全防护

网络

终端

移动

虚拟化

云

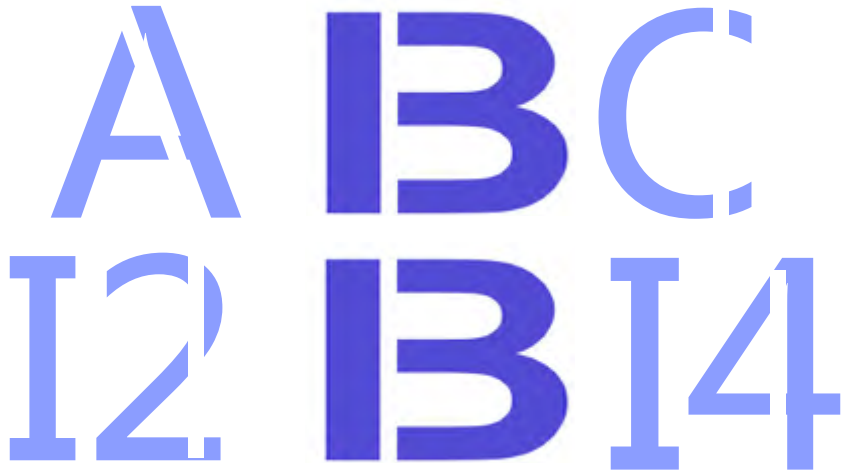
# 网络可见性——同时需要广度和深度

# 利用情景感知技术提供全面可见性

在网络内部

**LOCAL**
Business Context

- Who
- What
- How
- Where
- When



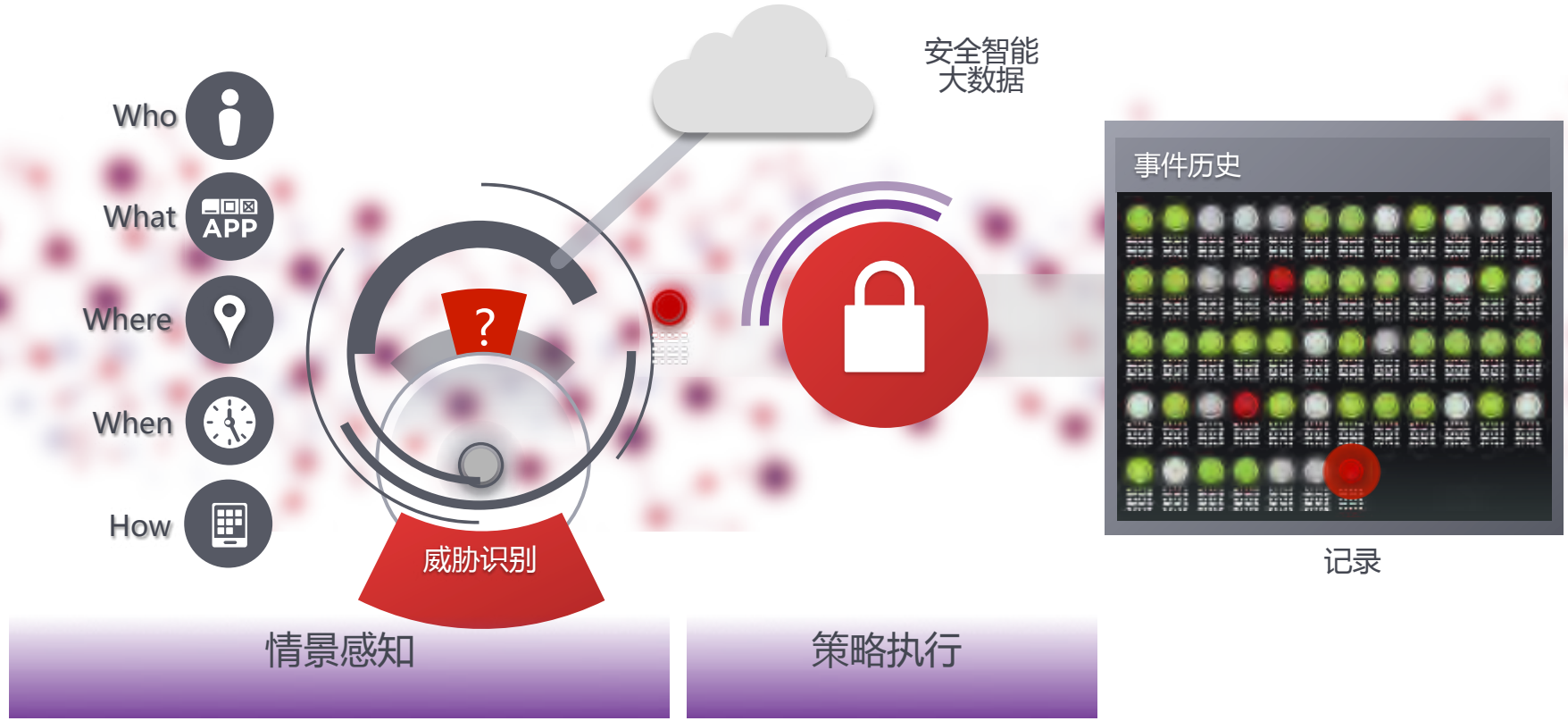

在网络外部

**GLOBAL**
Situational
Threat Intelligence

- Reputation
- Interactions
- Applications
- Sites

# 关注威胁

# 检测、阻止、理解威胁



# 持续的高级威胁防御


情景感知

策略执行

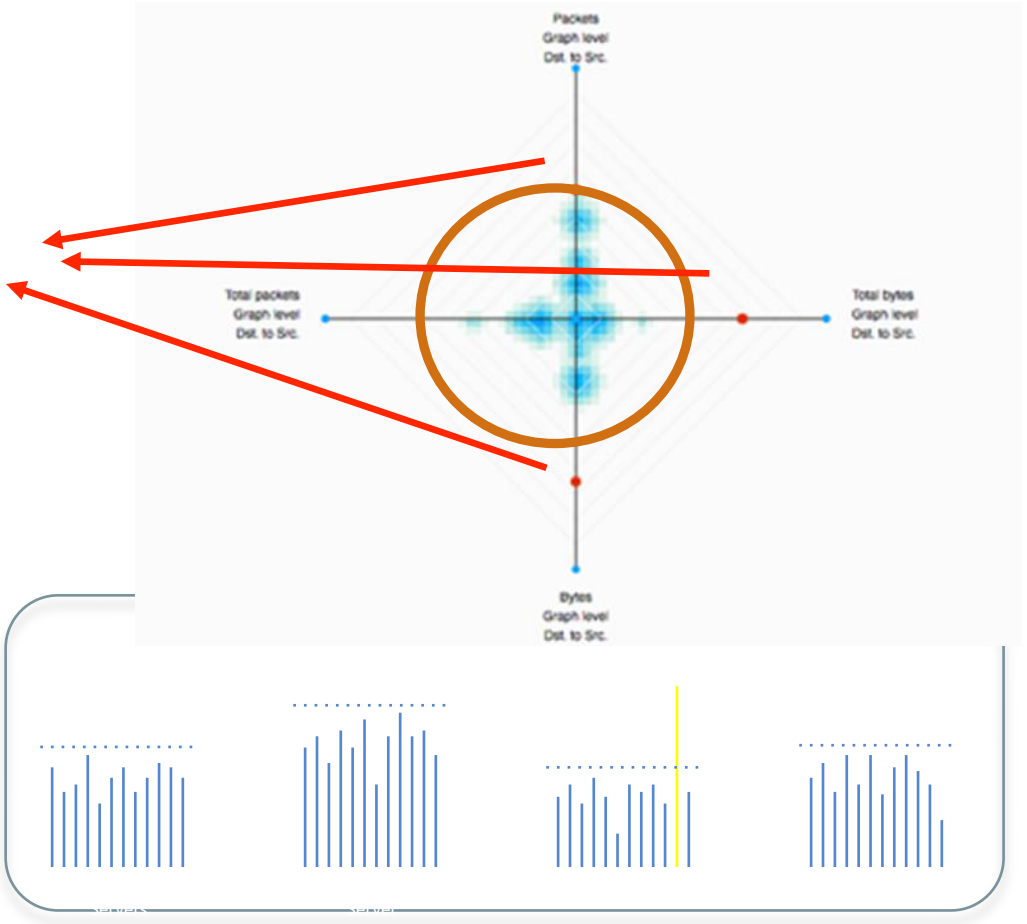
持续分析

# 关键技术：全球化的安全情报

# 关键技术：本地大数据与机器学习

网络与应用大数据分析/机器学习

- 安全性
- 性能表现
- 异常流量



# 网络基础平台可以为安全做出更多

攻击前
发现
执行
加固

攻击中
监测
阻断
防御

攻击后
定位
缓解
修复

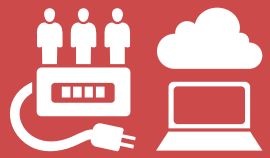
## 细粒度隔离

减少横向移动
加强动态细粒度控制，合规

## 网络作为传感器

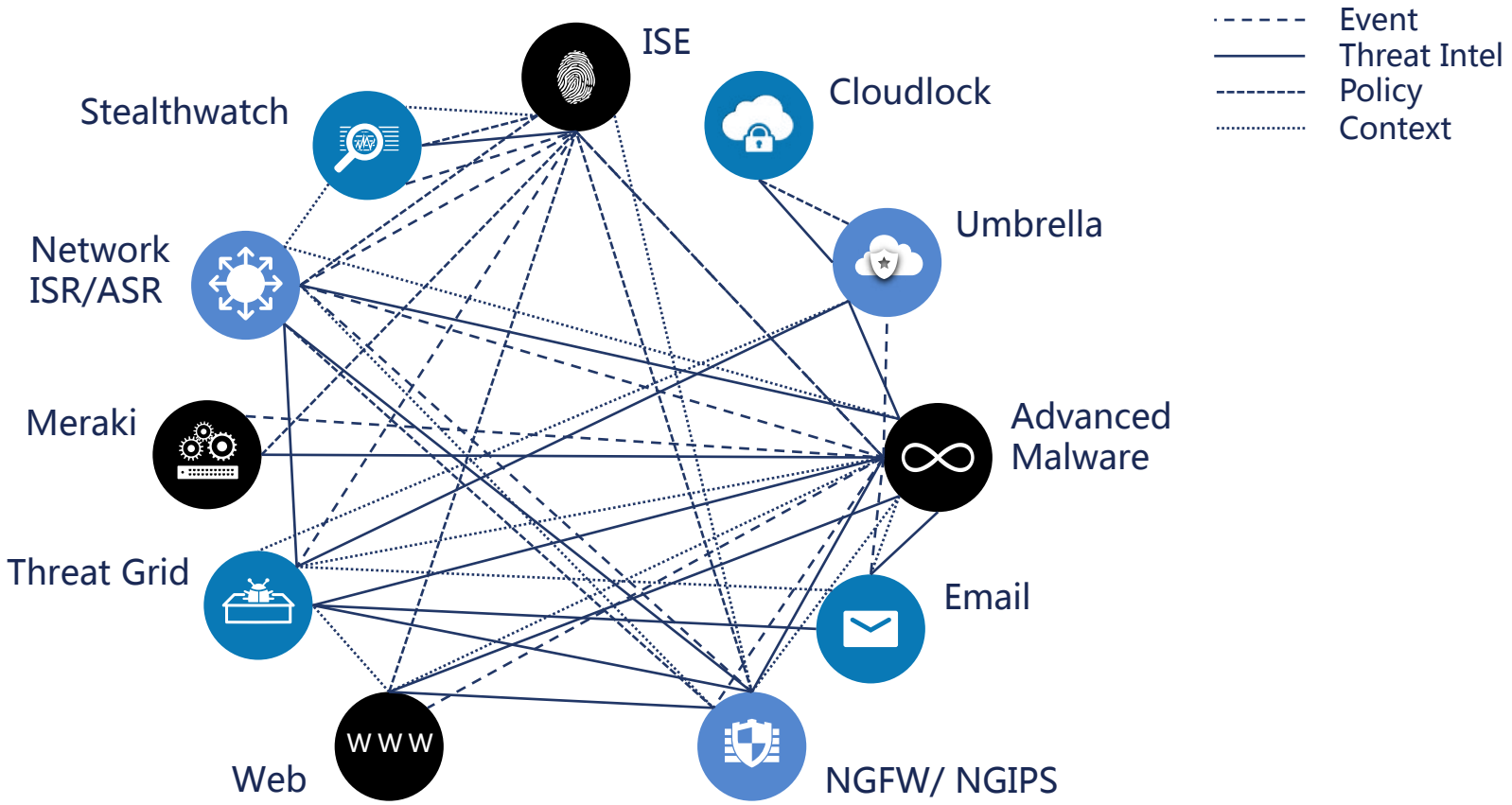
监测异常信息流
恶意设备及应用，以及用户的使用违规现象

## 快速缓解

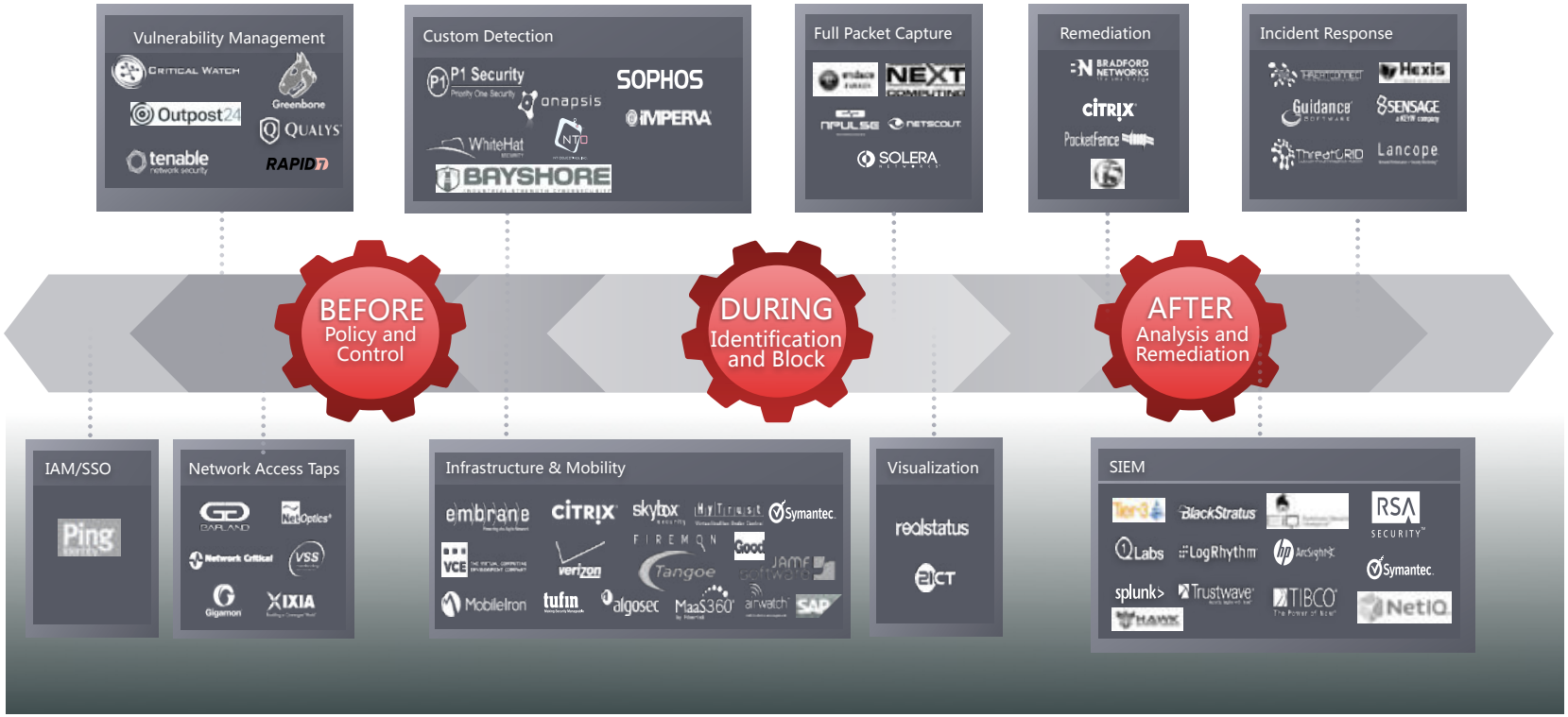


自动隔离
流量重定向
实时应用控制

# 思科技术实现信息共享,高效安全



# 统一平台，整合业界力量




WOTA
51CTO
Thank you !