运用CDN构建网络安全护城河

马俊

Akamai 中国

Web 事业部高级售前技术专家

网络安全受到前所未有的关注与重视

“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。”

Akamai FASTER FORWARD

互联网安全

攻击的态势

防护的趋势

Akamai的优势

Akamai FASTER FORWARD

互联网安全

攻击的态势

防护的趋势

Akamai的优势

Attack Categories, Last Hour

68.23% SQL Injection
393,812

26.99% Remote File Inclusion
155,760

4.32% PHP Injection
24,946

0.46% Cross-Site Scripting
2,658

0.00% Command Injection
6

数据规模 | 8千万条/小时WAF规则被触发 | 60万行日志/秒 | **超过**20 TB/日新增攻击流量

分析 | **全球专职的资深安全专家团队** | 每日处理超过8,000 个安全工单

12,139,260
Web Application Attacks,
Last 24 Hours

Akamai

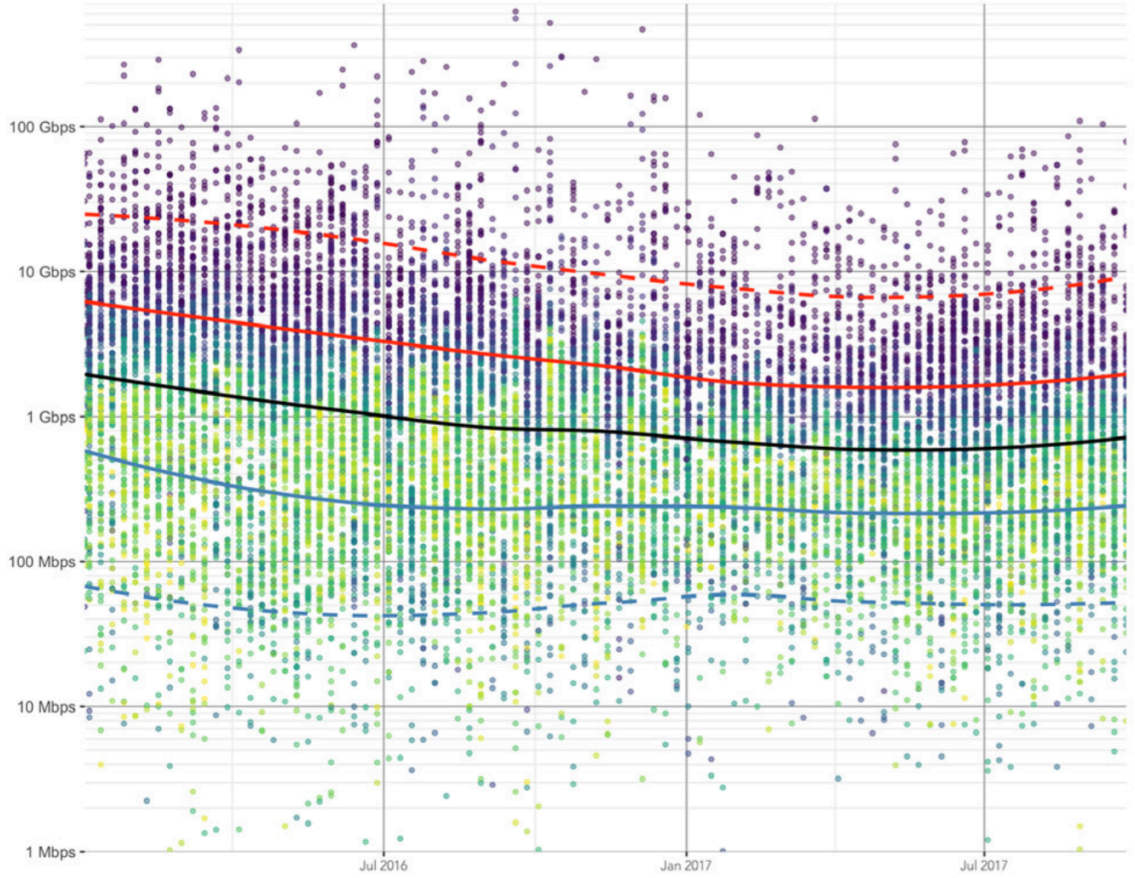
http://wwwnui.akamai.com/gnet/globe/index.html

攻击数据（DDoS攻击）

Q3 2017	Q2 2017	Q1 2017	Q4 2016	Q3 2016
109 Gbps	75 Gbps	120 Gbps	517 Gbps	623 Gbps

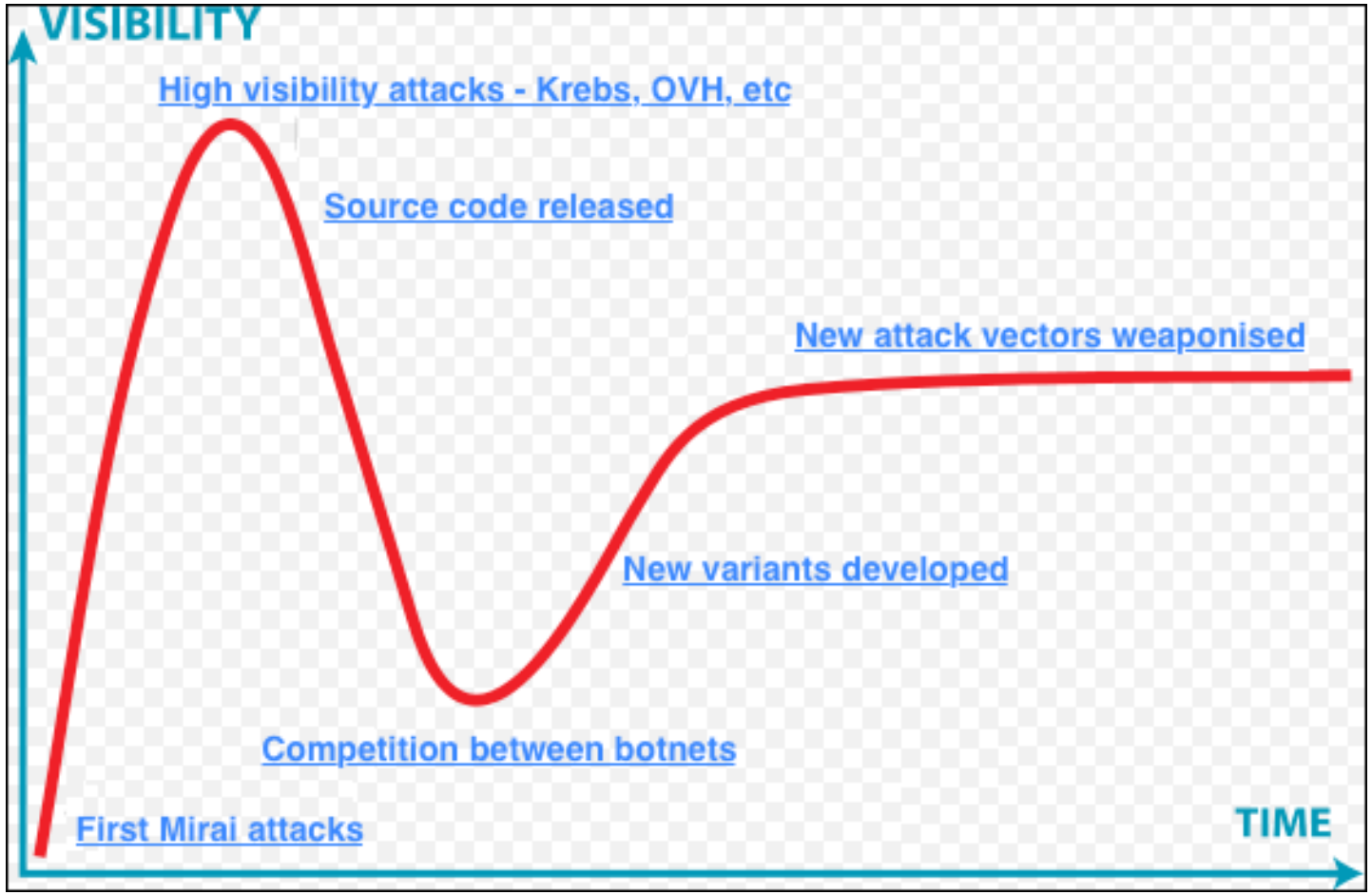
如果您的网络拥有 8.8 Gbps 带宽（含日常流量）可以保护及应对约 95% 的互联网DDoS攻击

如果您的网络拥有 1.8 Gbps 带宽（含日常流量）可以保护及应对约 75% 的互联网DDoS攻击



攻击数据（DDoS攻击）

Q3 2017	Q2 2017	Q1 2017	Q4 2016	Q3 2016
109 Gbps	75 Gbps	120 Gbps	517 Gbps	623 Gbps



攻击数据（应用攻击）

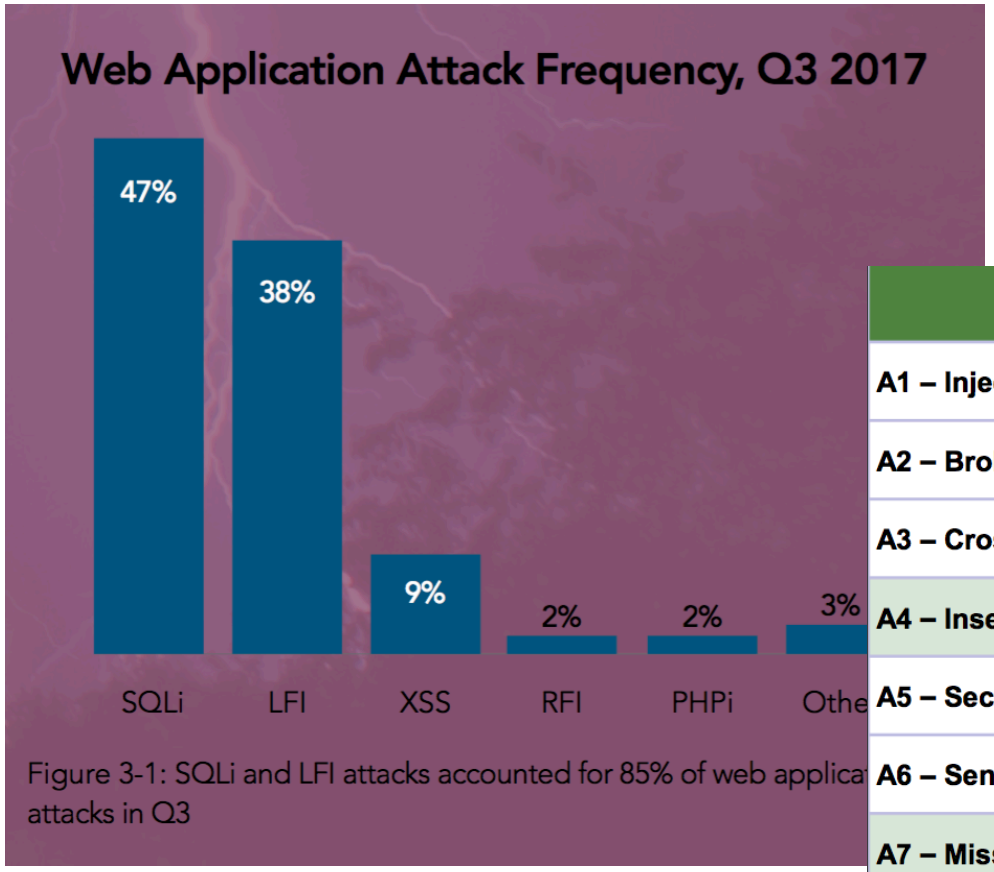


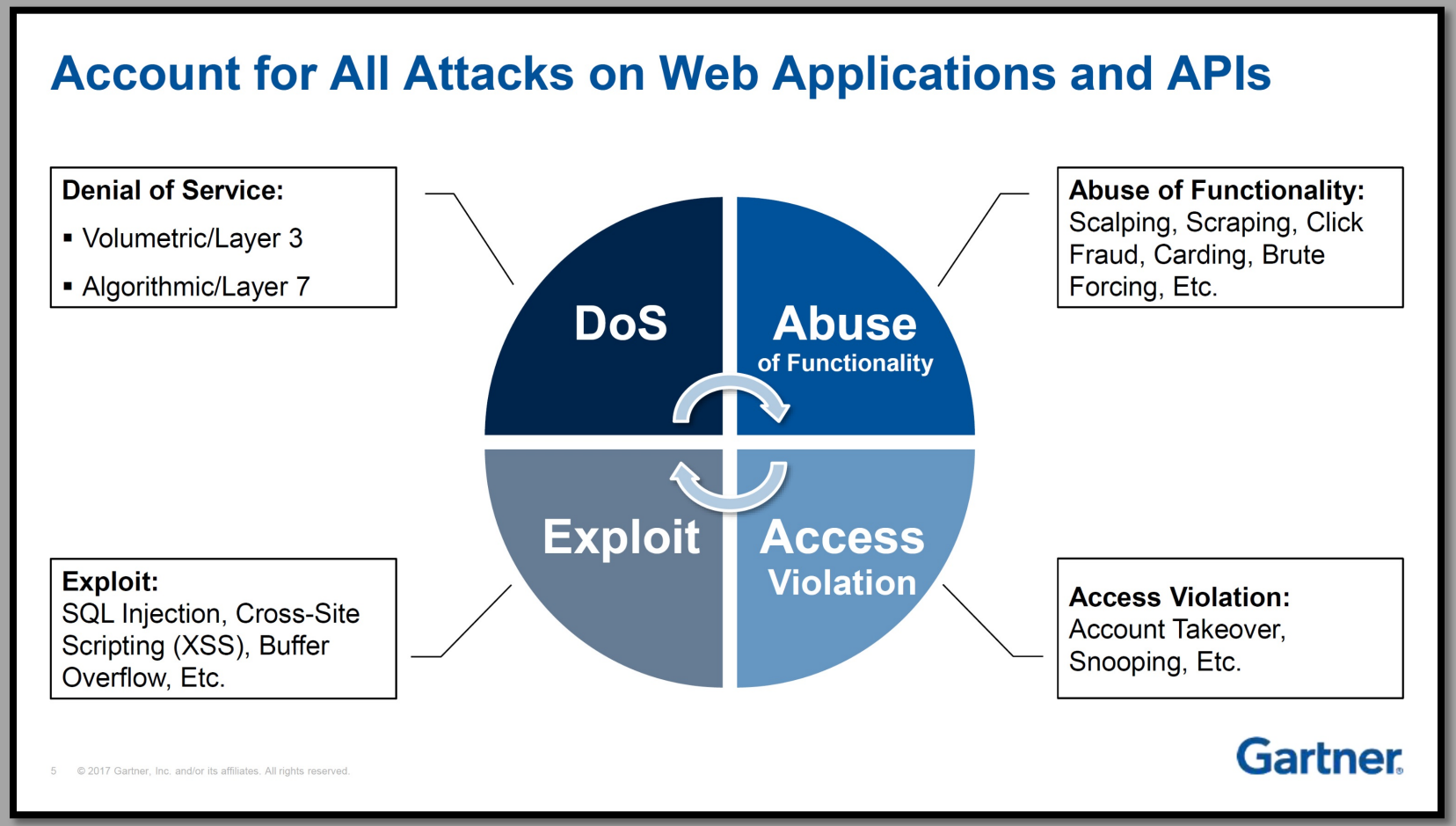
Figure 3-1: SQLi and LFI attacks accounted for 85% of web applica attacks in Q3

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

主要攻击方式

DDoS
3层：大流量规模
7层：算法与逻辑

漏洞
SQL注入、跨站、缓冲区溢出等



Gartner Security & Risk Management Summit Presentation, State of Application Security, Ramon Krikken, June 2017

功能滥用
短时攻击、搜取攻击、点击欺诈、信用卡盗刷、暴力破解等

访问盗用
撞库、监听等

144.7B

HTTP 次请求

每天的 HTTP 流量中

35%

AJAX, Web类, 以及其他

65%

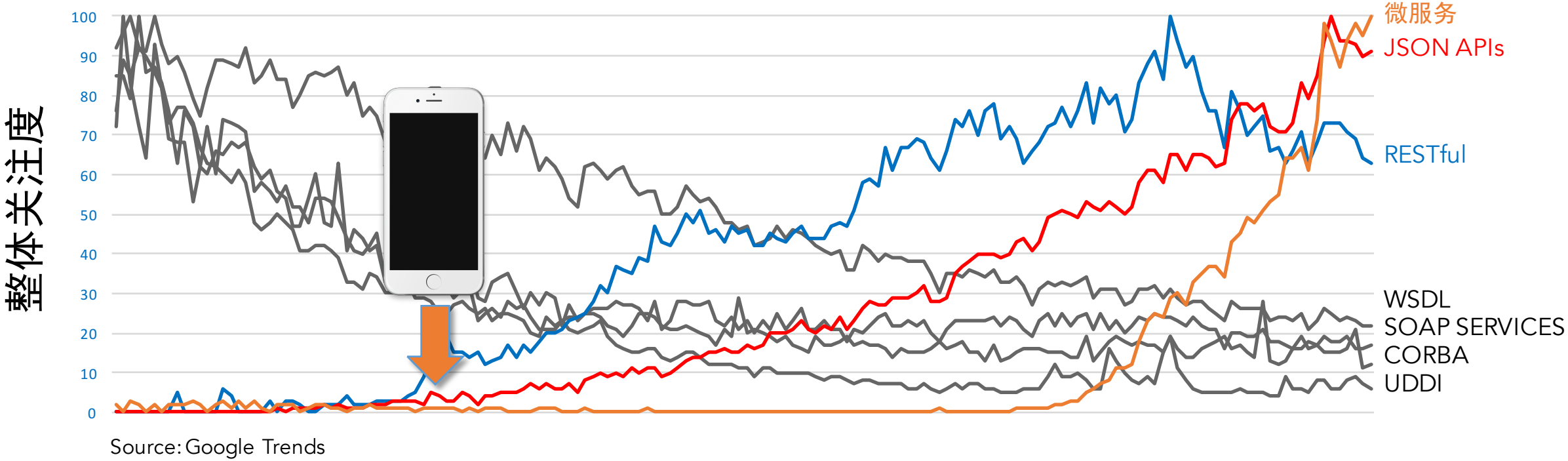
移动端 APIs

36.6B

API 调用

25% 的流量是API的流量

API技术爆发的过程



Source: Google Trends

API安全防护的技术难度很高！

Gartner

Page Rule Settings

Incapsula blocking my mobile app requests, how do I bypass this?

asked by The Cook on Feb 03 2017 07:15

we are using Incapsula for web security in our application. It works fine for web.

However, Incapsula blocks all mobile application requests (iOS:Swift, Android:Java) ; and classifies them as `DDOS` and `CAPTCHA (Fail)` with status messages:

`Client was sent a JavaScript security check, request was suspended`

or

`Client was sent a CAPTCHA security check, request was suspended`.

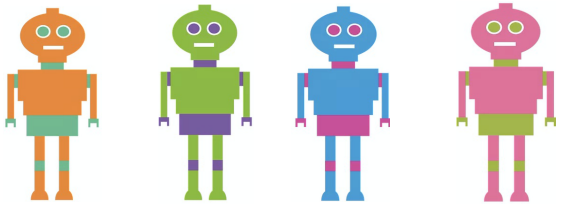
How do I bypass this?

I am using Asynchronous Http Client for Android, Alamofire for iOS.

integrity check for the API URL pattern so that calls made outside of a browser are not blocked.

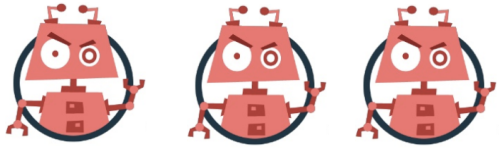
其他顶级的安全厂商在API的防护场景中都有严重的误报！

爬虫的“两难境地”



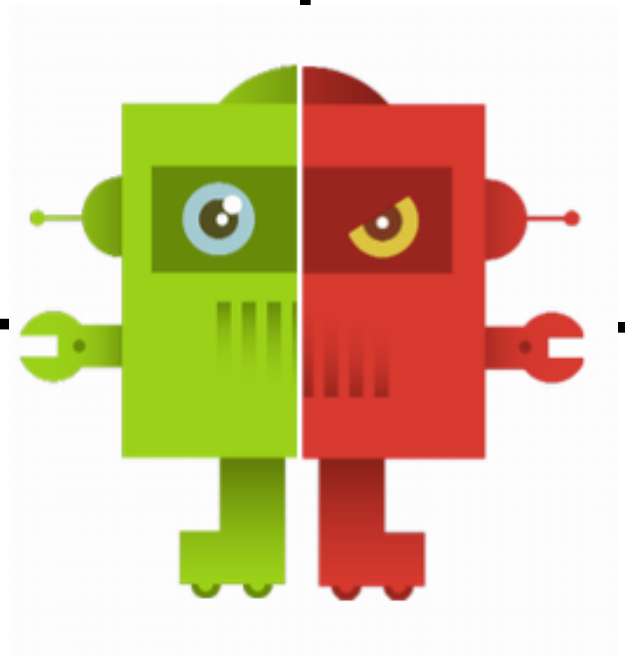
好

坏



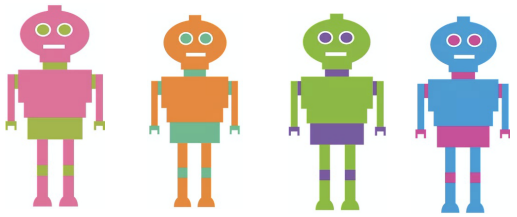
已知

未知



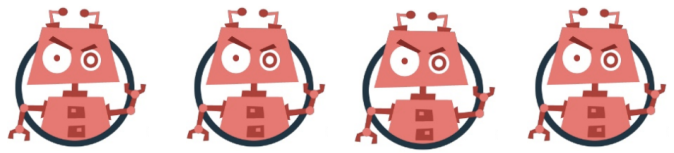
已知

未知

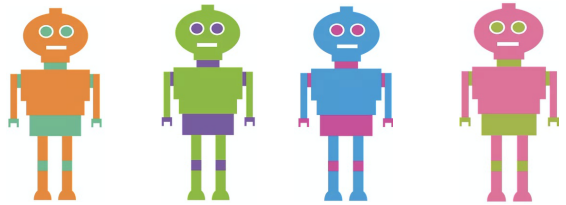


好

坏

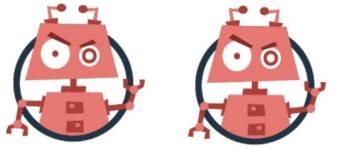


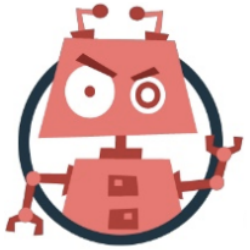
爬虫的运动趋势



好

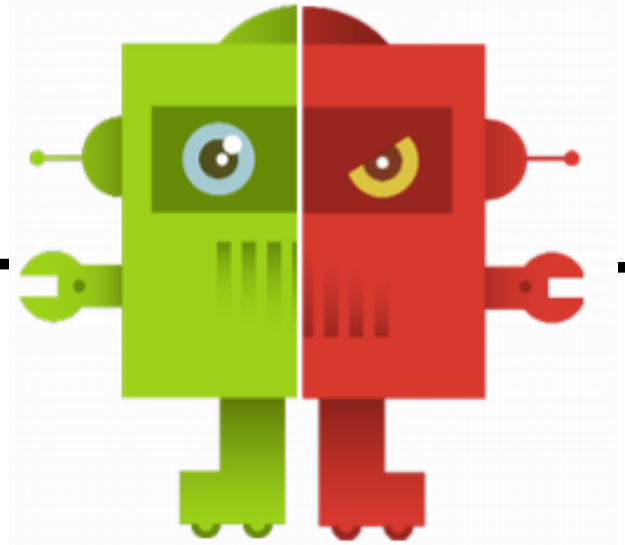
坏





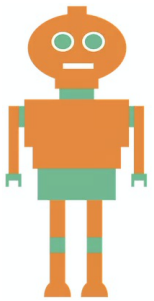
已知

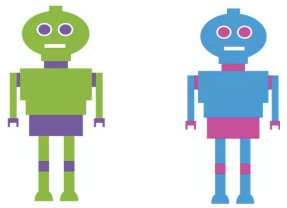
未知



已知

未知



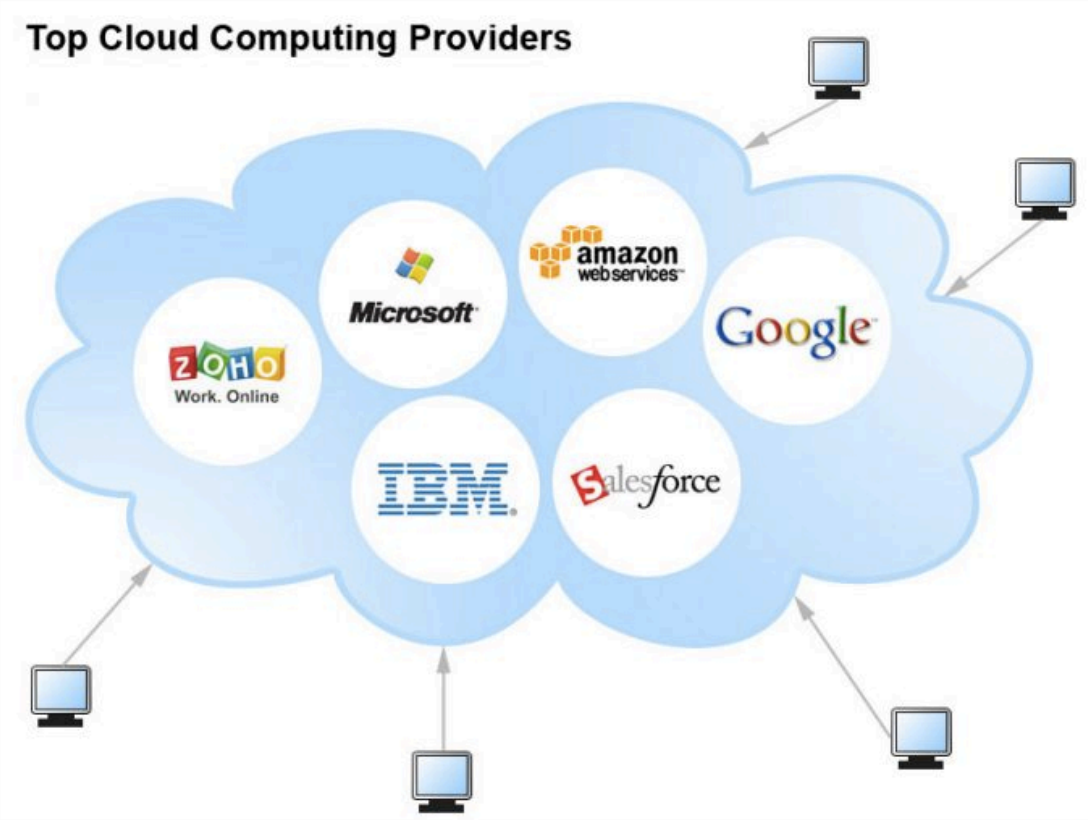


好

坏

爬虫的运动趋势

- **越来越容易**： 60s 建一个爬虫网络？



WebSpider.py - C:\Python32\WebSpider.py

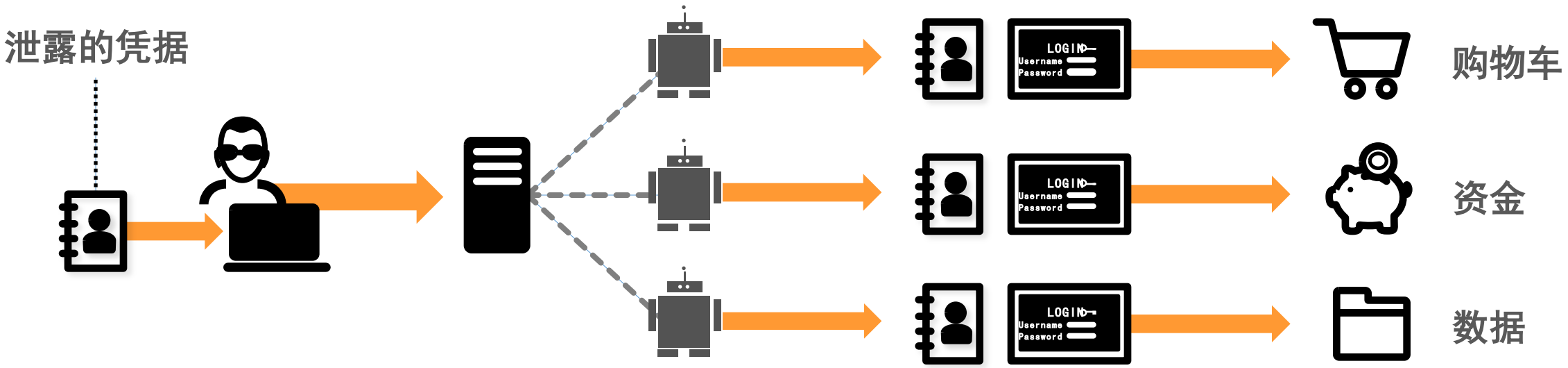
File Edit Format Run Options Windows Help

```
from html.parser import HTMLParser
from urllib.request import urlopen
from urllib import parse

class LinkParser(HTMLParser):

    def handle_starttag(self, tag, attrs):
        if tag == 'a':
            for (key, value) in attrs:
                if key == 'href':
                    newUrl = parse.urljoin(self.baseUrl, value)
                    self.links = self.links + [newUrl]

    def getLinks(self, url):
        self.links = []
        self.baseUrl = url
        response = urlopen(url)
        if response.getheader('Content-Type')=='text/html':
            htmlBytes = response.read()
            htmlString = htmlBytes.decode("utf-8")
            self.feed(htmlString)
            return htmlString, self.links
        else:
            return "",[]

def spider(url, word, maxPages):
    pagesToVisit = [url]
    numberVisited = 0
    foundWord = False
    while numberVisited < maxPages and pagesToVisit != [] and not foundWord:
        numberVisited = numberVisited +1
        url = pagesToVisit[0]
        pagesToVisit = pagesToVisit[1:]
        try:
            print(numberVisited, "Visiting:", url)
            parser = LinkParser()
            data, links = parser.getLinks(url)
            if data.find(word)>-1:
                foundWord = True
            pagesToVisit = pagesToVisit + links
            print(" **Success!**")
        except:
            print(" **Failed!**")
    if foundWord:
        print("The word", word, "was found at", url)
    else:
        print("Word never found")
```

Ln: 47 Col: 33

撞库攻击

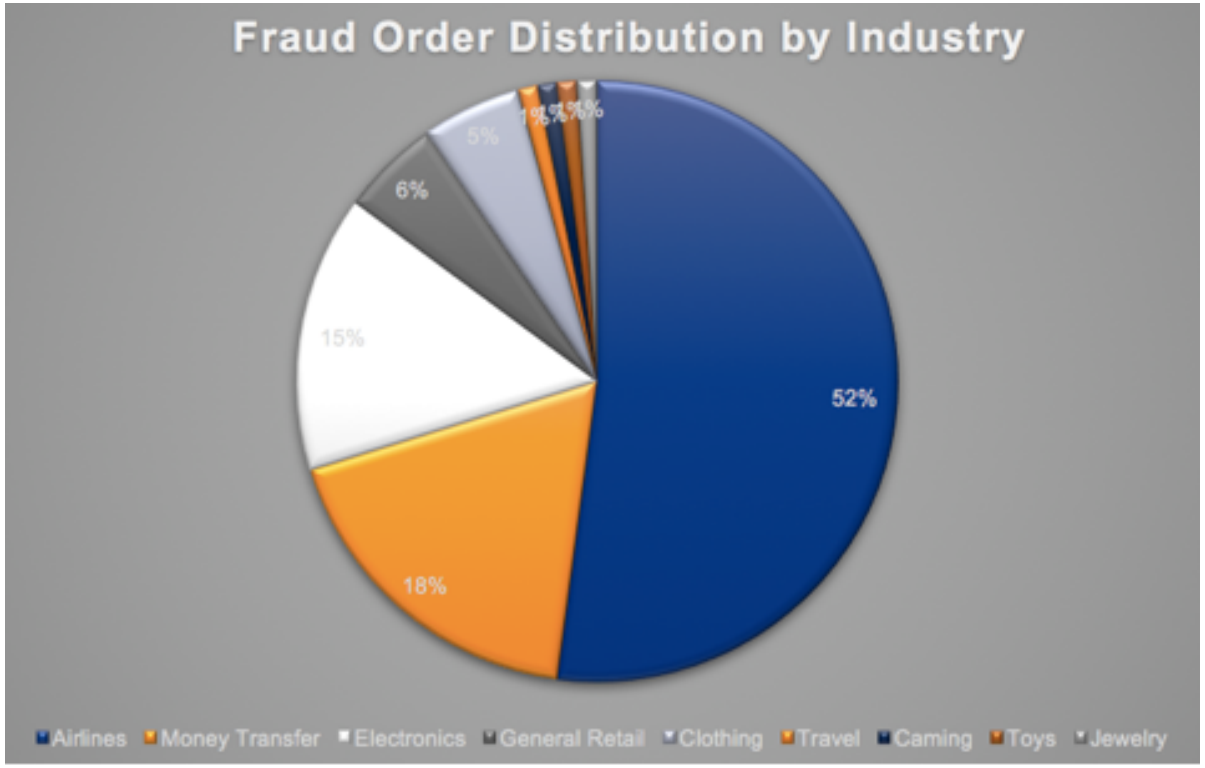
黑产批量购买凭据	验证凭据	登录	攻击目标



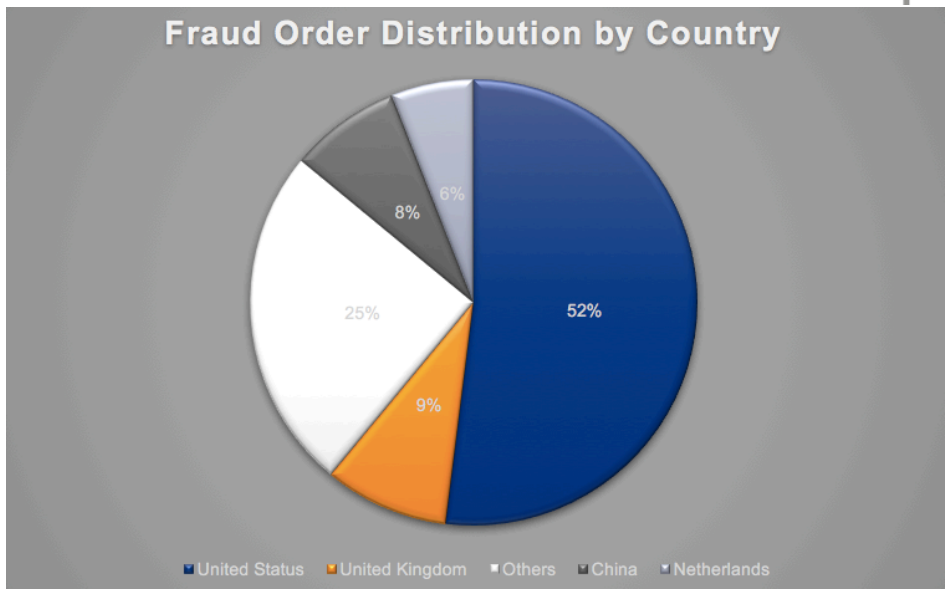
欺诈者	BOTNET	网站	用户的信息资产

爬虫的运动趋势

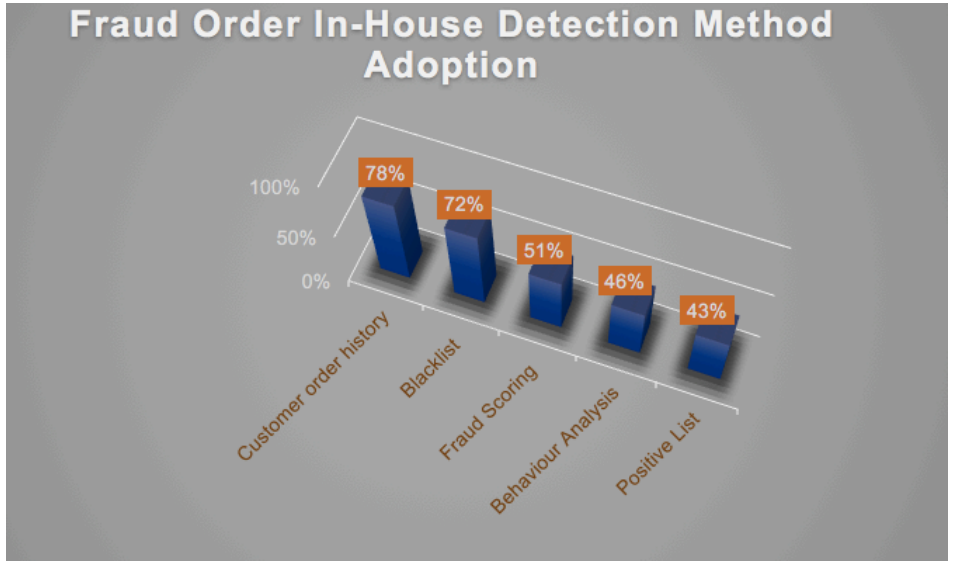
业务影响 – *爬虫下订单*



欺诈订单的行业分布



欺诈订单的国家分布



欺诈订单的本地检查方法

Akamai FASTER FORWARD

互联网安全

攻击的态势

防护的趋势

Akamai的优势

构架外部安全防护体系

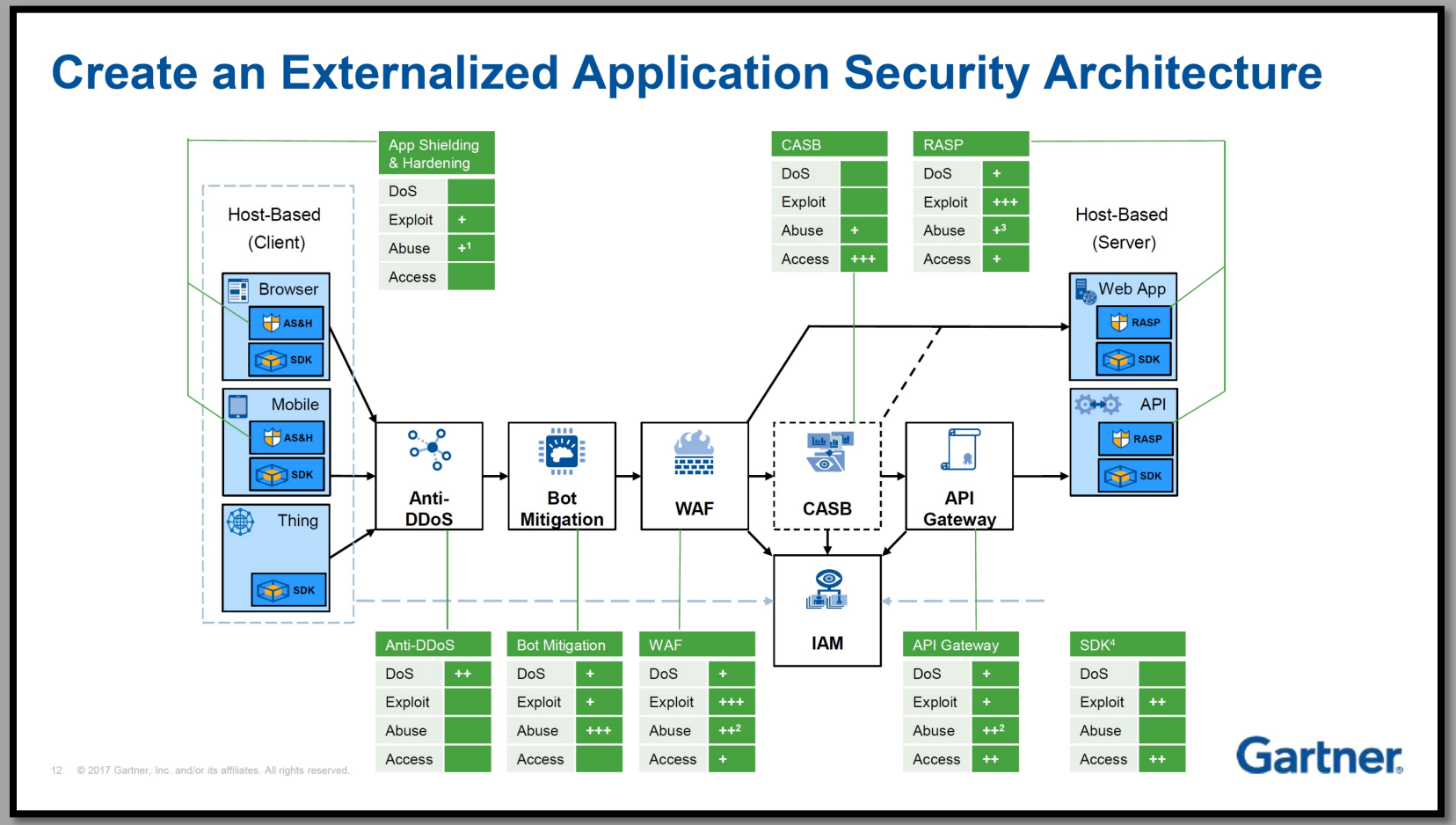
DDoS防护

反爬虫

应用防火墙

外部身份认证

API 网关



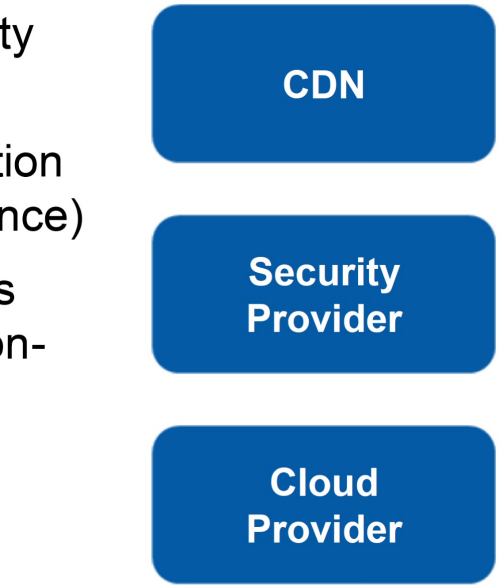
Gartner Security & Risk Management Summit Presentation, State of Application Security, Ramon Krikken, June 2017

Gartner建议

- 外部安全优先考虑云安全
- DDoS、威胁过滤是云安全的优势
- 混合的架构（云+现场）

Implement Cloud-Based and Hybrid Security Architecture

- Use scalability and scale of cloud-based security providers and infrastructure … think cloud first
- Use cloud-based components for threat protection in particular (DDoS, threat filtering and intelligence)
- Consider hybrid architecture for single functions (e.g., DDoS), or to split functions (e.g., to add on-premises data protection)

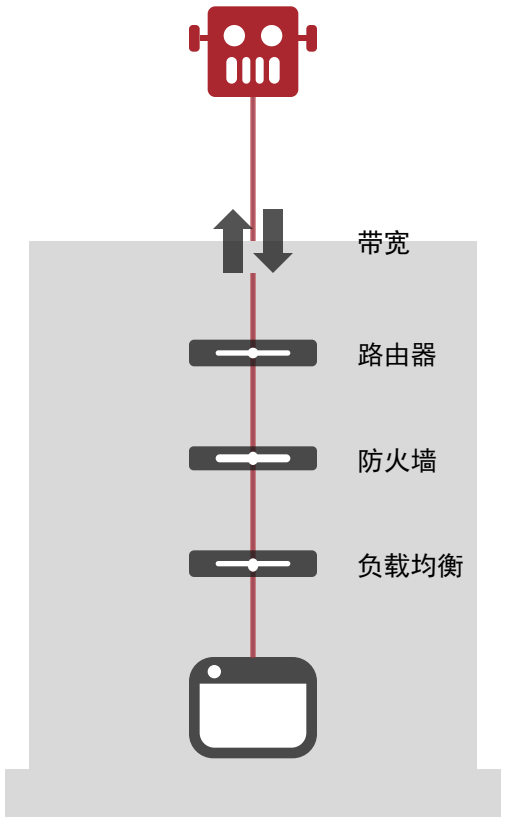


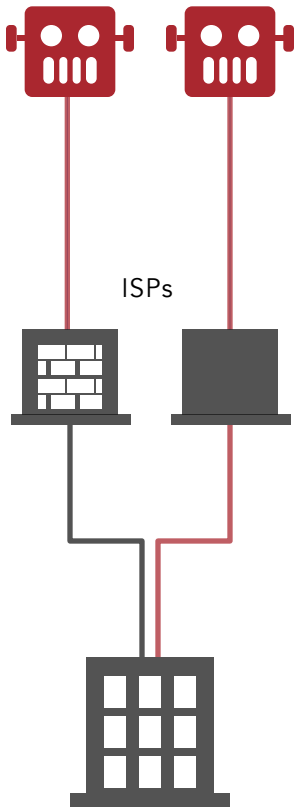
Gartner

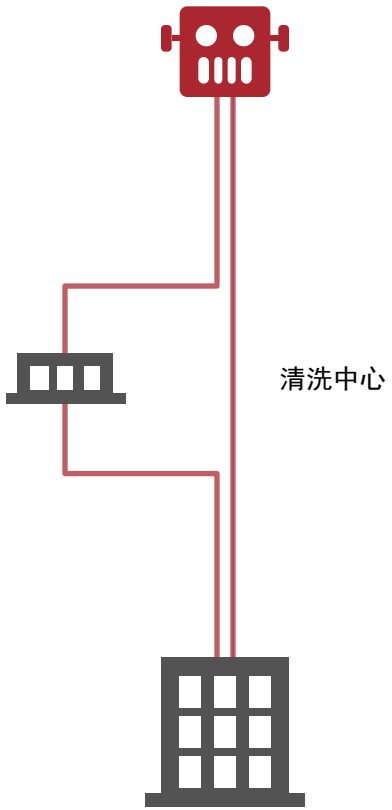
Gartner Security & Risk Management Summit Presentation, State of Application Security, Ramon Krikken, June 2017

防护方案对比

现场部署设备	ISP/网络运营商	清洗中心	云端防护

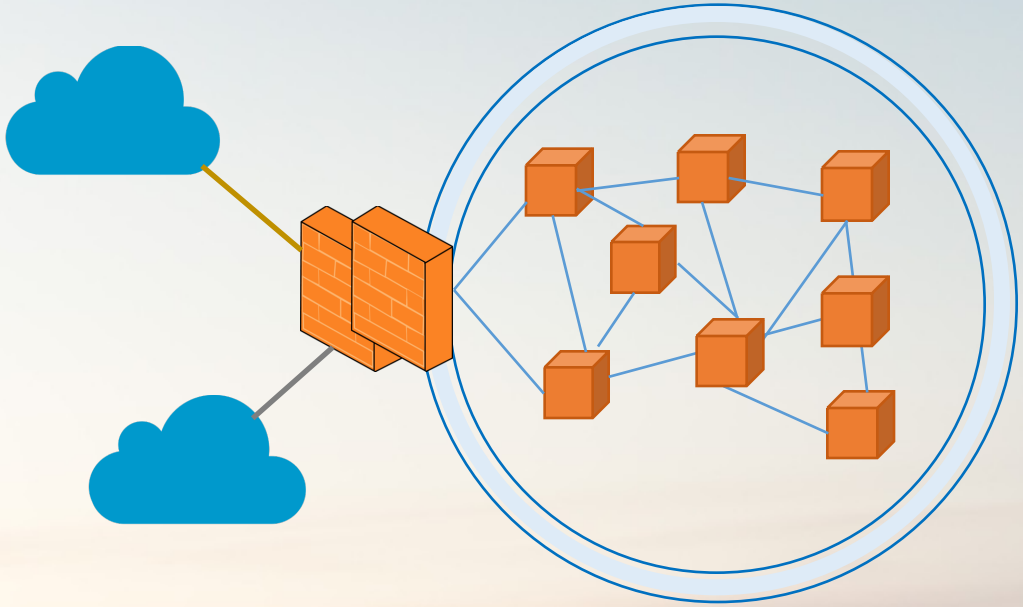






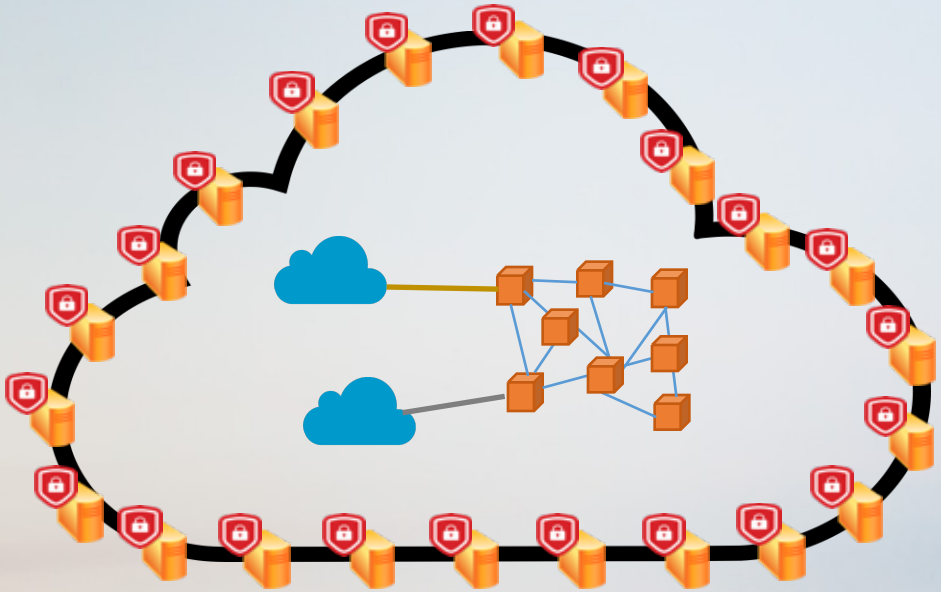
Akamai 为基于云的架构体系提供云原生的安全特性

- 传统的“堡垒和护城河”不再适用；
- 您的应用程序、数据和用户均已在防火墙以外！



传统的安全边界与架构

- Akamai 将安全策略放置在互联网的边界；
- 轻而易举的为云时代提供安全防护！



Akamai 云安全

Akamai FASTER FORWARD

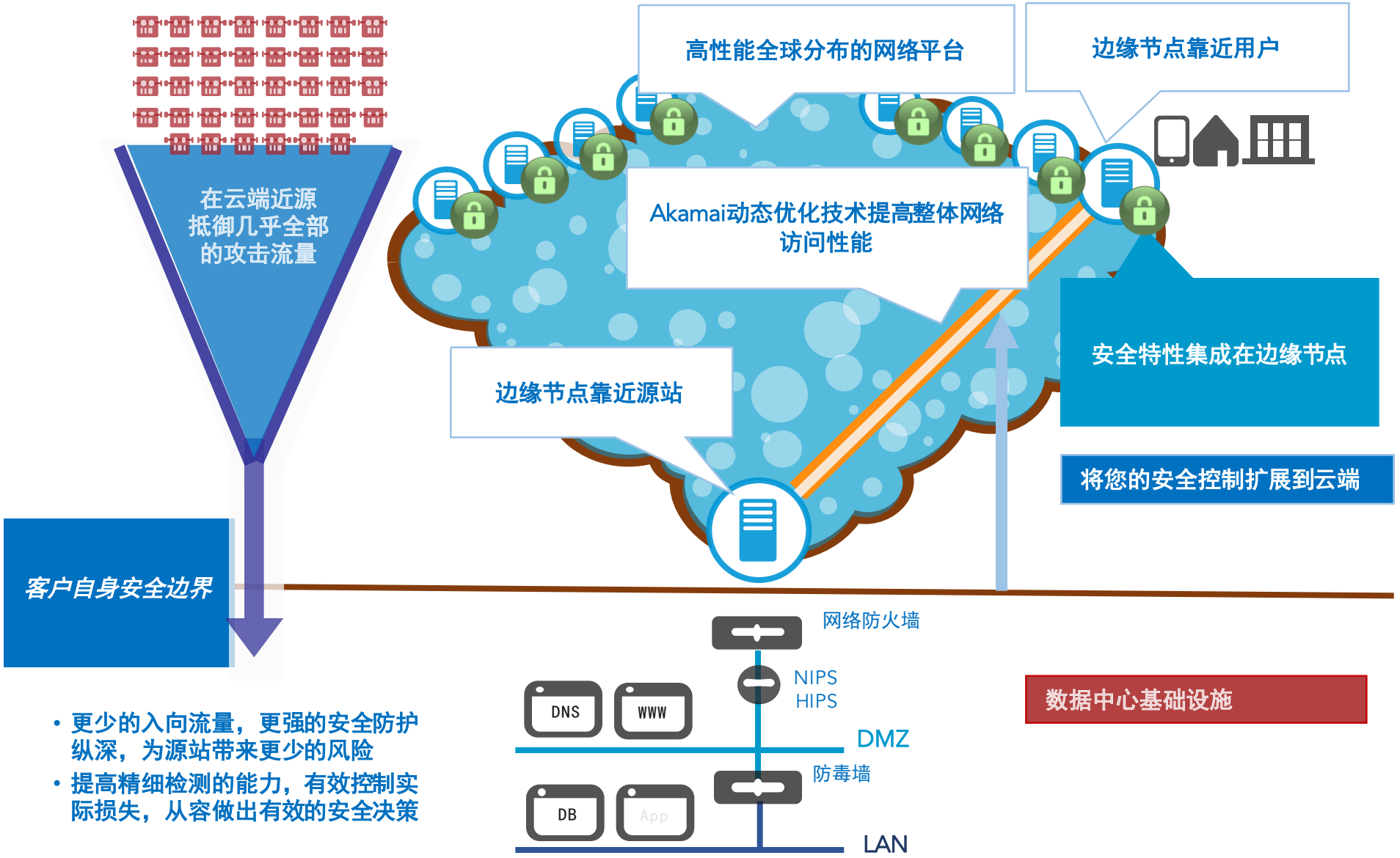
互联网安全

攻击的态势

防护的趋势

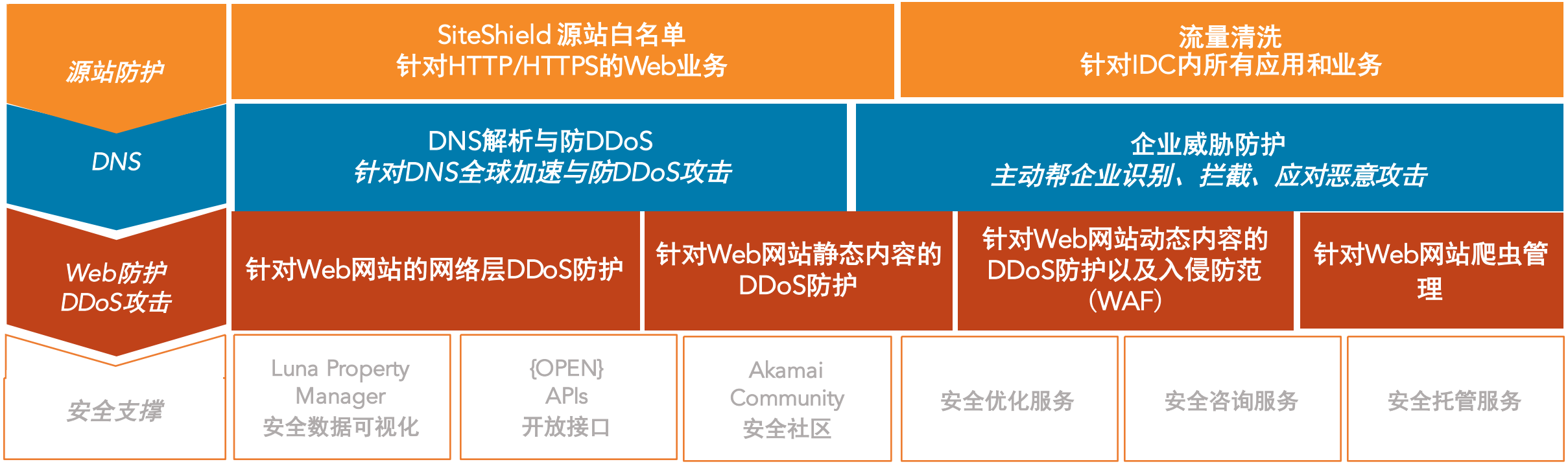
Akamai的优势

Akamai云安全与数据中心安全边界



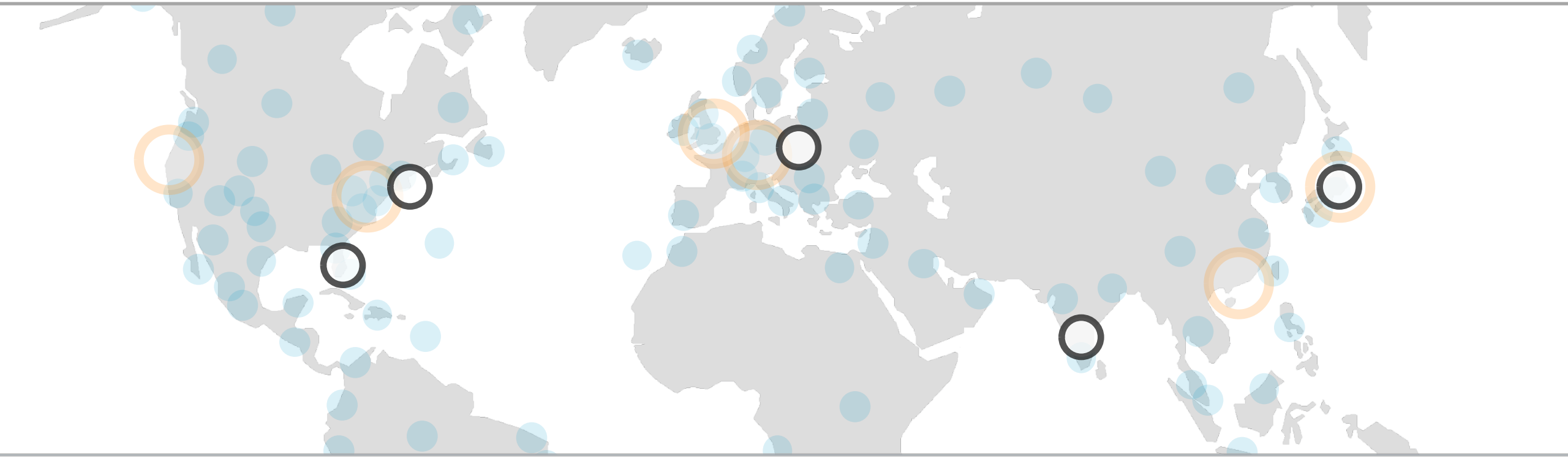
- 更少的入向流量，更强的安全防护纵深，为源站带来更少的风险
- 提高精细检测的能力，有效控制实际损失，从容做出有效的安全决策

Akamai 整体安全防护体系



平台规模

Akamai安全支持



全球5个安全应急中心SOC | 7个流量清洗中心

24x7 提供监控与应急响应服务

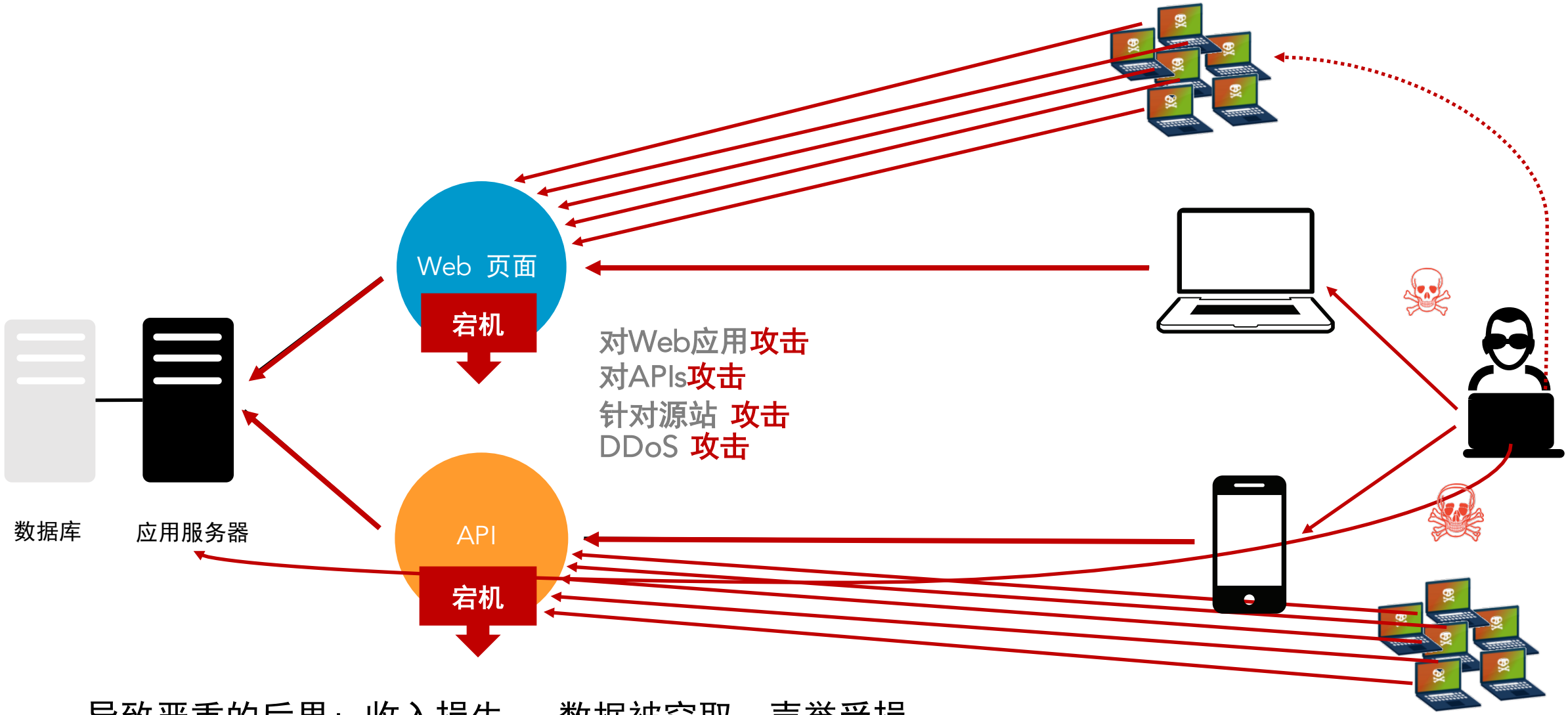
SOC | 美国劳德代尔堡 | 美国剑桥 | 波兰克拉科夫 | 印度班加罗尔 | 日本东京

清洗中心 | 美国圣何塞 | 美国阿什本 | 英国伦敦 | 德国法兰克福 | 日本东京 | 中国香港 | 澳大利亚悉尼

Gartner 将 Akamai 置于最新发布的 2017 Web 应用防火墙魔力象限评估中

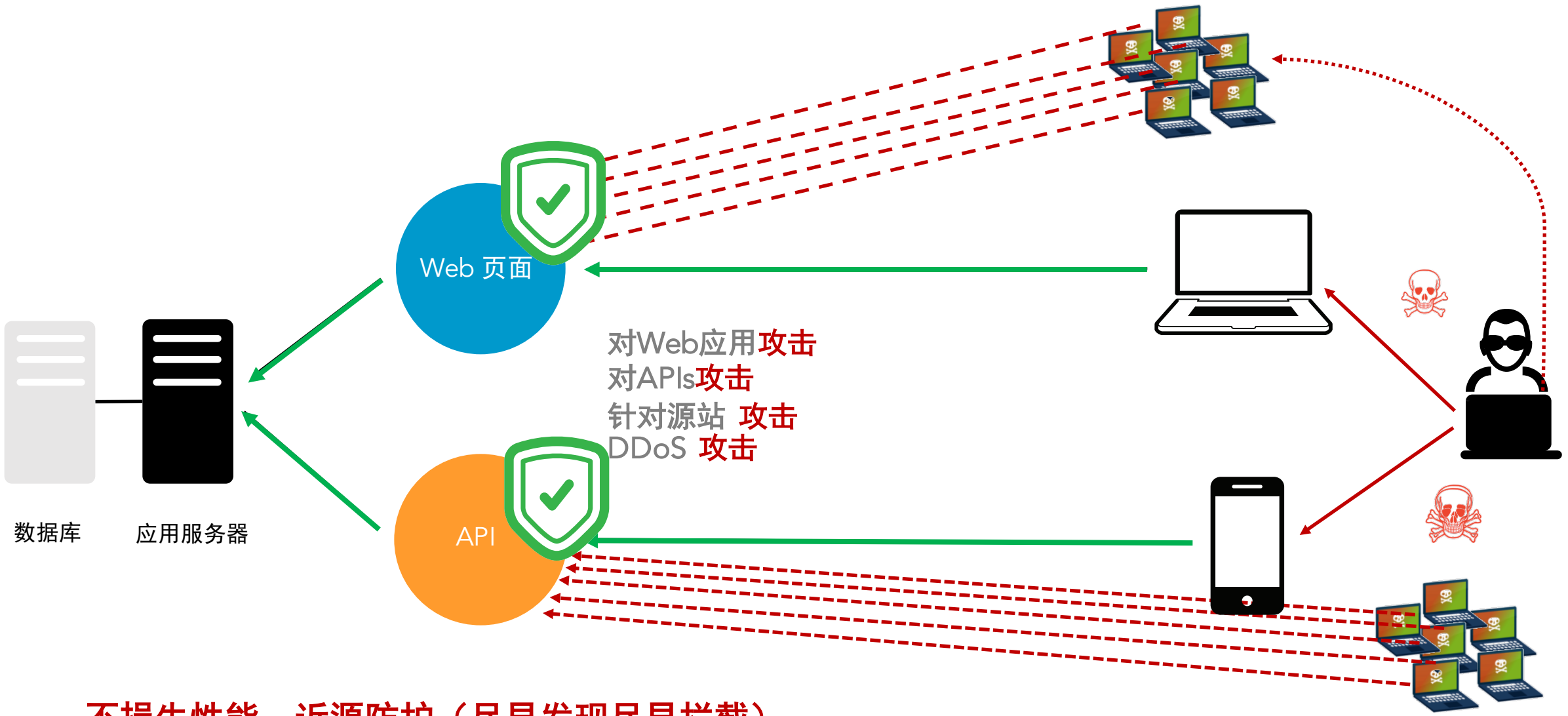
Gartner, Magic Quadrant for Web Application Firewalls, 07 August 2017

攻击方式



导致严重的后果：收入损失， 数据被窃取，声誉受损

云端防护

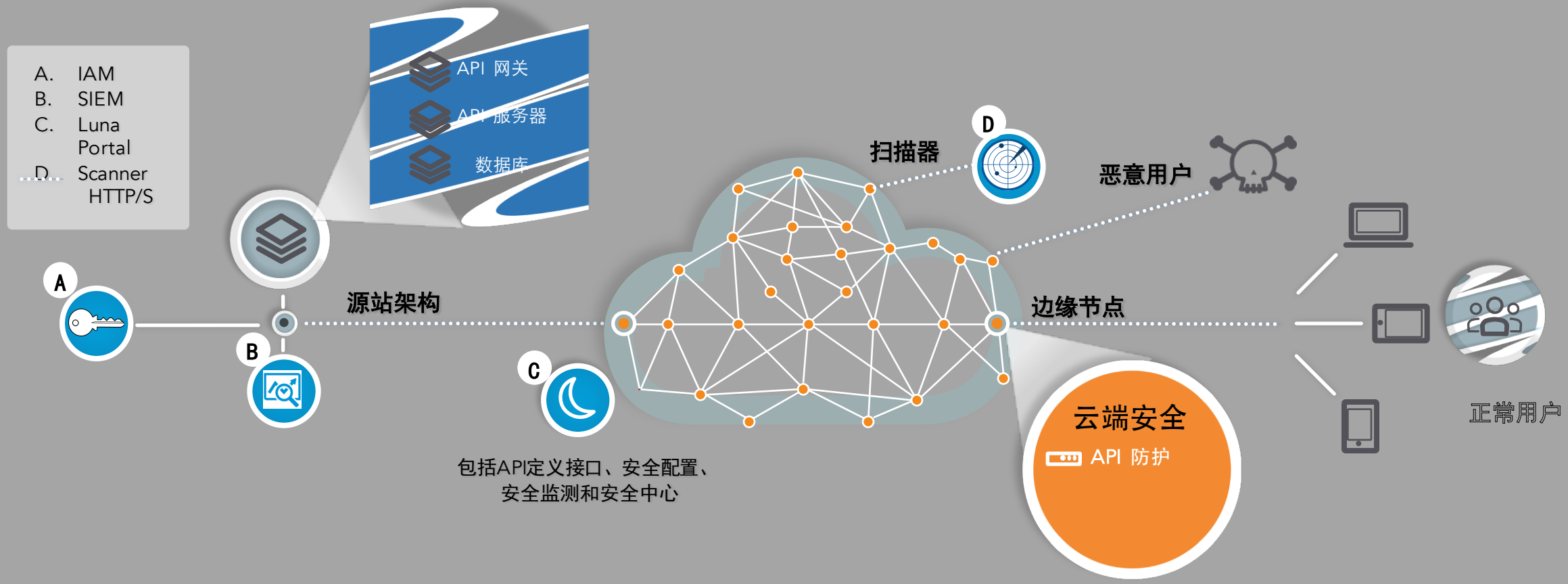


不损失性能，近源防护（尽早发现尽早拦截）

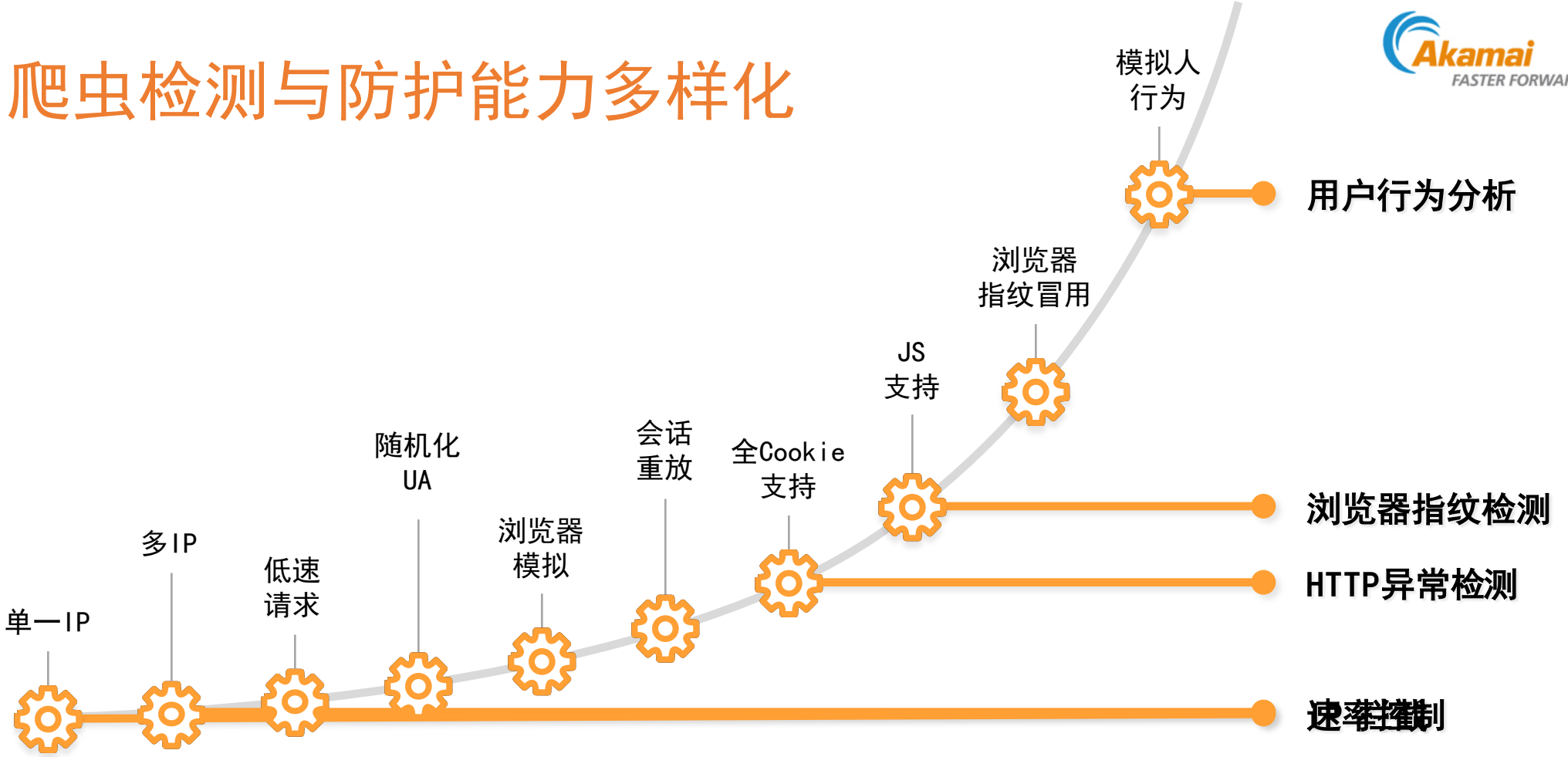
Akamai API 防护优势

JSON/XML 检测	主动 安全模型	强化的速率控制 和 慢速POST保护	网络层保护	分析与报表	云平台
发现并拦截对已知API漏洞的探测与利用	定义“正常” 对“异常”进行报警与拦截	快速响应轻易解决利用API进行的定向DDoS攻击	IP/地理位置 黑白名单	在API层面进行事件响应与漏错报调优	应对海量API流量时保证扩展性

Akamai API 防护架构



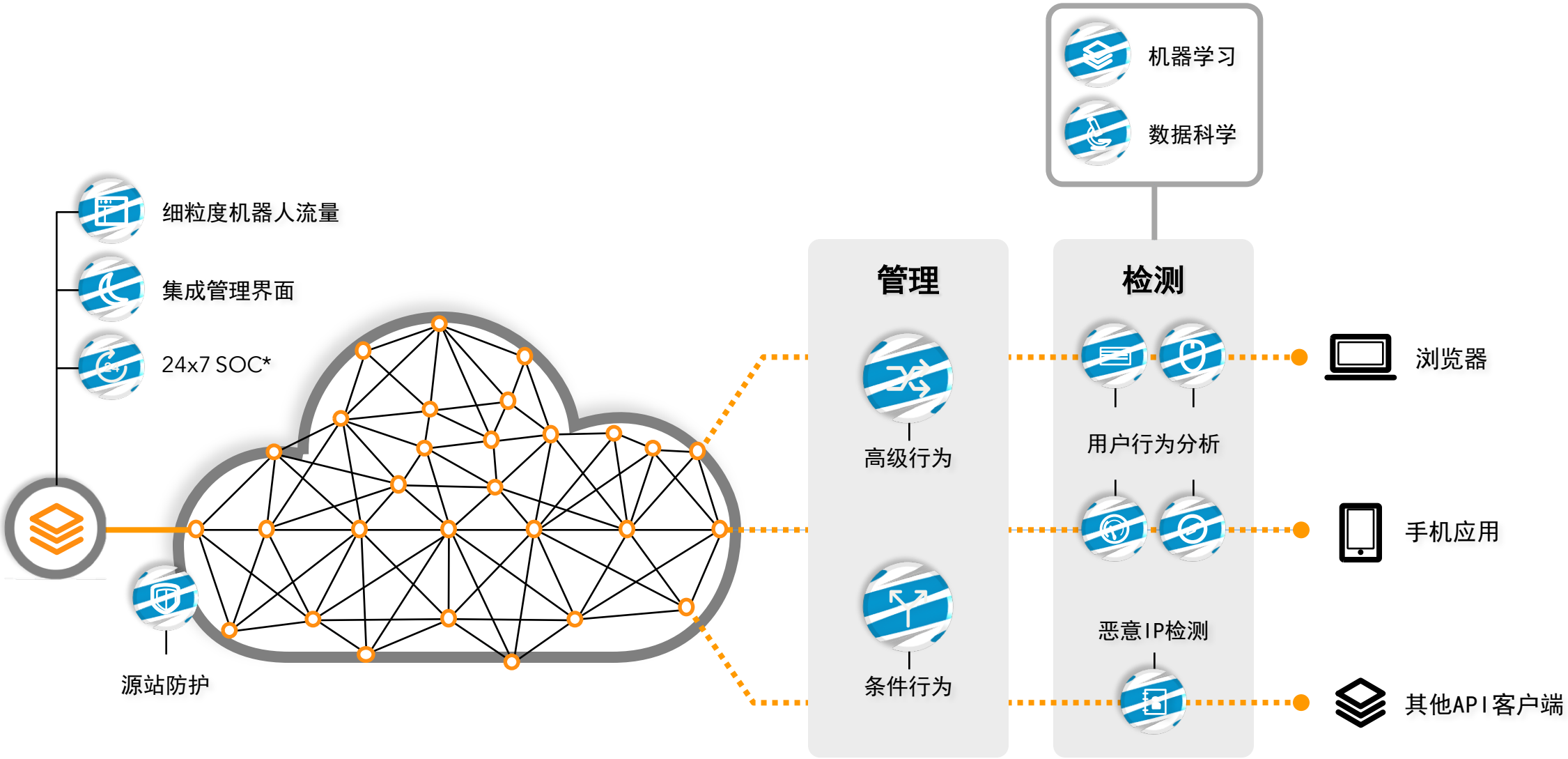
爬虫检测与防护能力多样化



简单 ——————————→ 越来越难

- Basic | 监控
  拦截
- Drop | 拦截
- Rate | 延缓 (1-3s)
  拖慢 (8-10s)
- Serve | 另外的源站
  另外的内容
  从缓存中交付

Akamai 爬虫治理架构

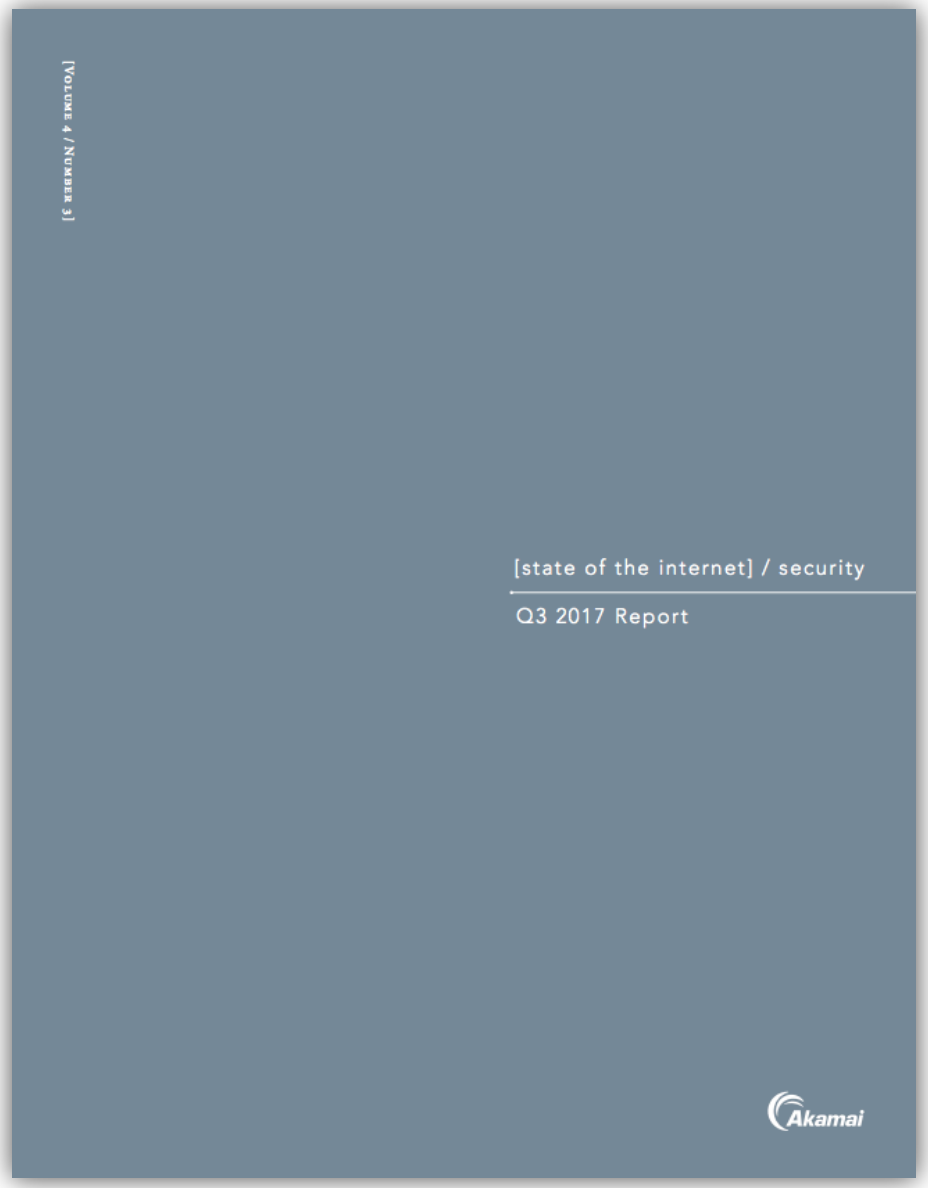


回顾与总结

网络攻击的发展超乎想象，立即采取措施才能让您的业务与系统安全可靠

Akamai 利用平台优势和服务优势帮助您在不影响性能的前提下提升整体安全性

Akamai被业界及用户广泛接受的方案在当前DDoS、API与爬虫等新攻击态势下能够让您的网站固若金汤

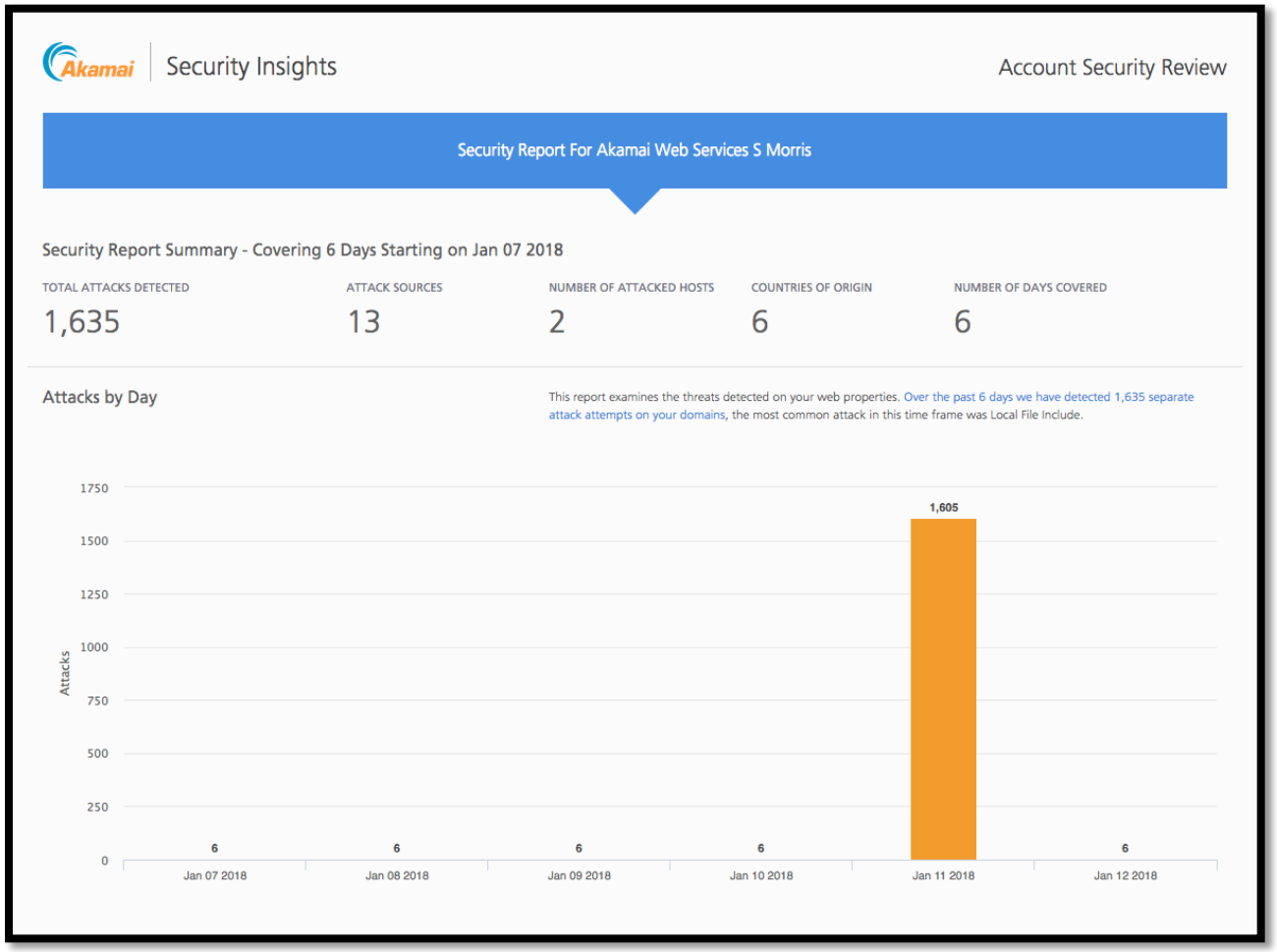


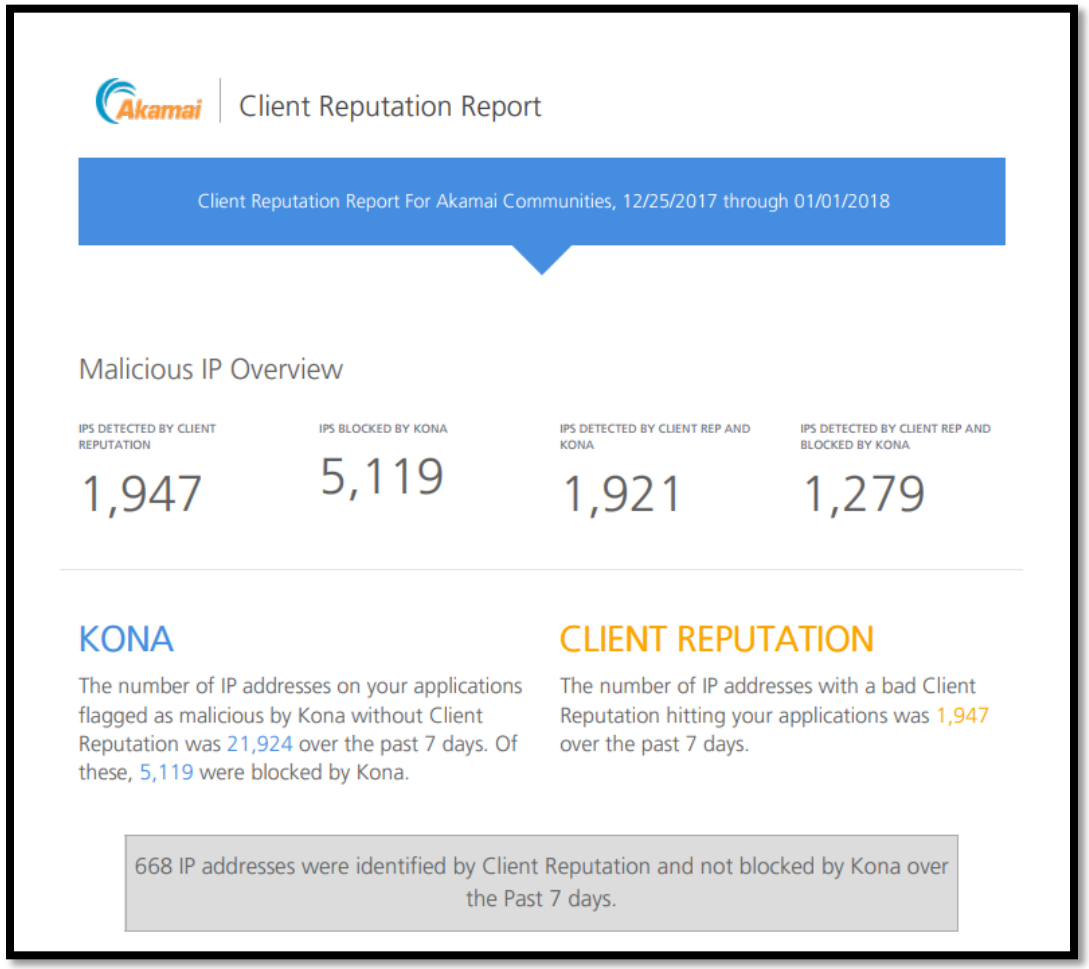
每季度发布全球互联网安全报告

报告详情可访问Akamai官网

http://akamai.com/soti

了解您自身的安全状态





Akamai加速平台的用户可以找您的售前工程师获取近7天的安全状态报告


Akamai
FASTER FORWARD
Akamai
FASTER FORWARD
IT大咖说
知识共享平台
THANK YOU