Akamai Security Summit World Tour

智能安全从边缘开始

保护企业免受互联网威胁的全新模式

Intelligent Security Starts at the Edge

智能安全从边缘开始
保护企业免受互联网威胁的全新模式

Nick Hawkins

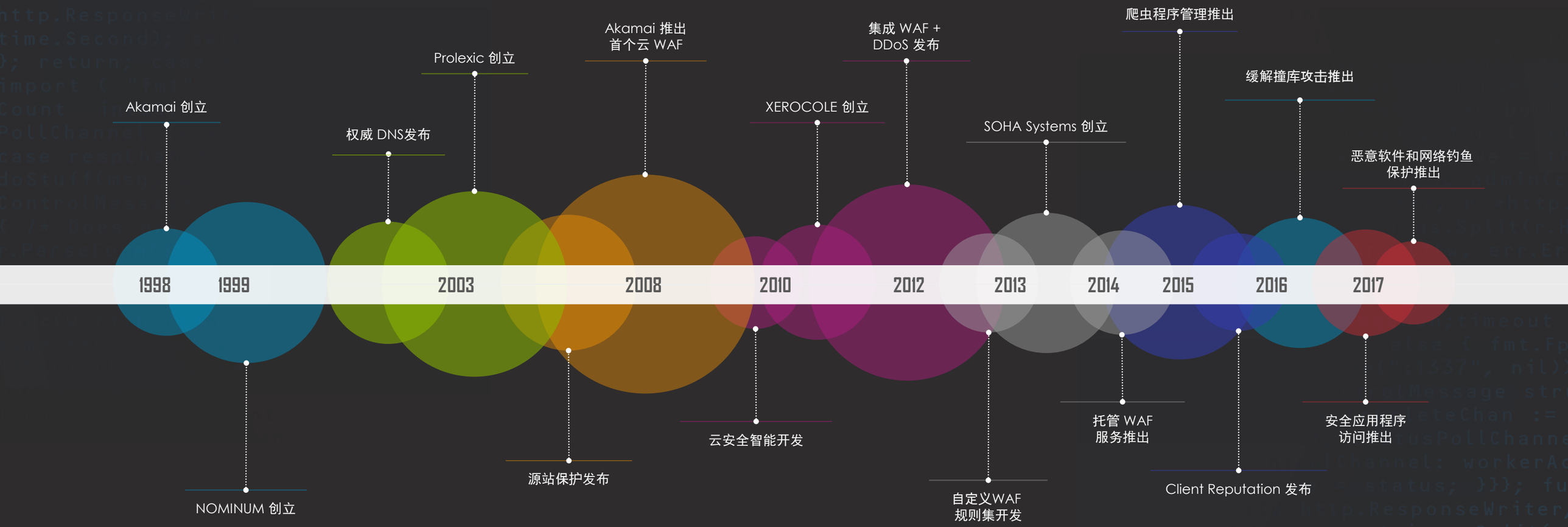
阿卡迈（Akamai）企业安全产品资深总监

Nick Hawkins

Senior Director of Enterprise Security Products

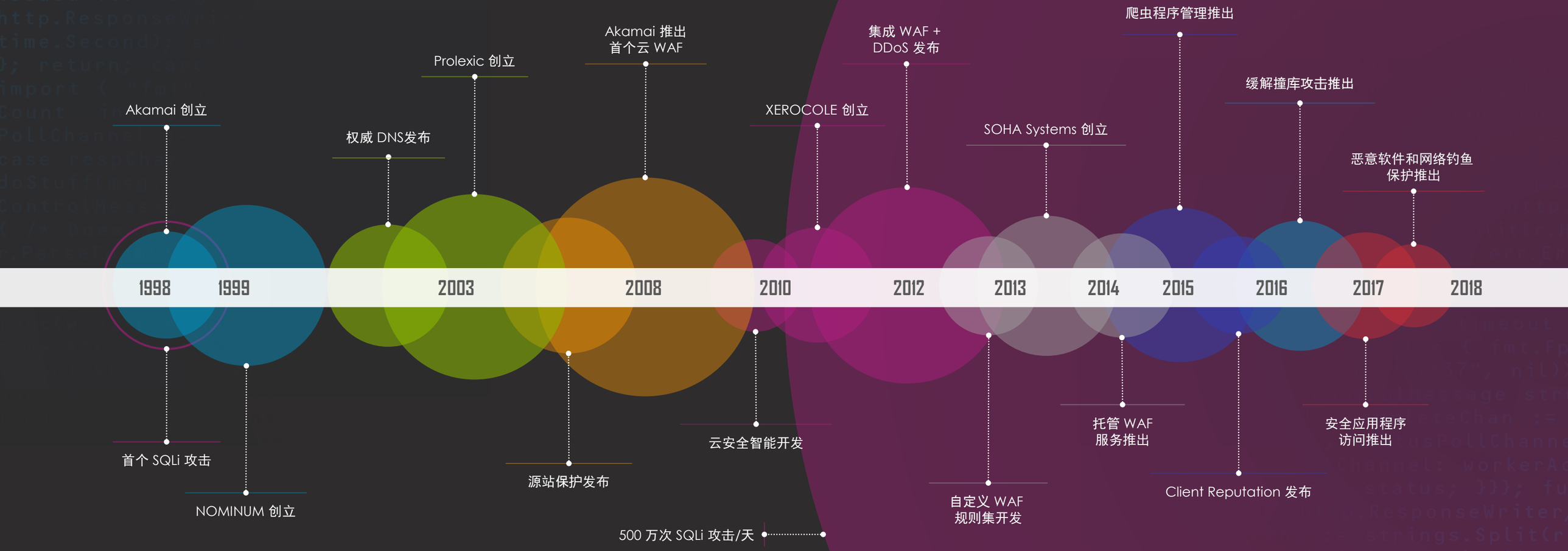
二十年安全行业经验

但安全性仍然是一项持久挑战



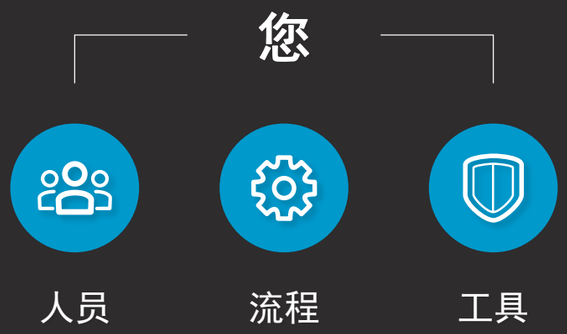
二十年安全行业经验

但安全性仍然是一项持久挑战



为什么安全防护如此困难？

一切都在变化，超越了您的响应速度

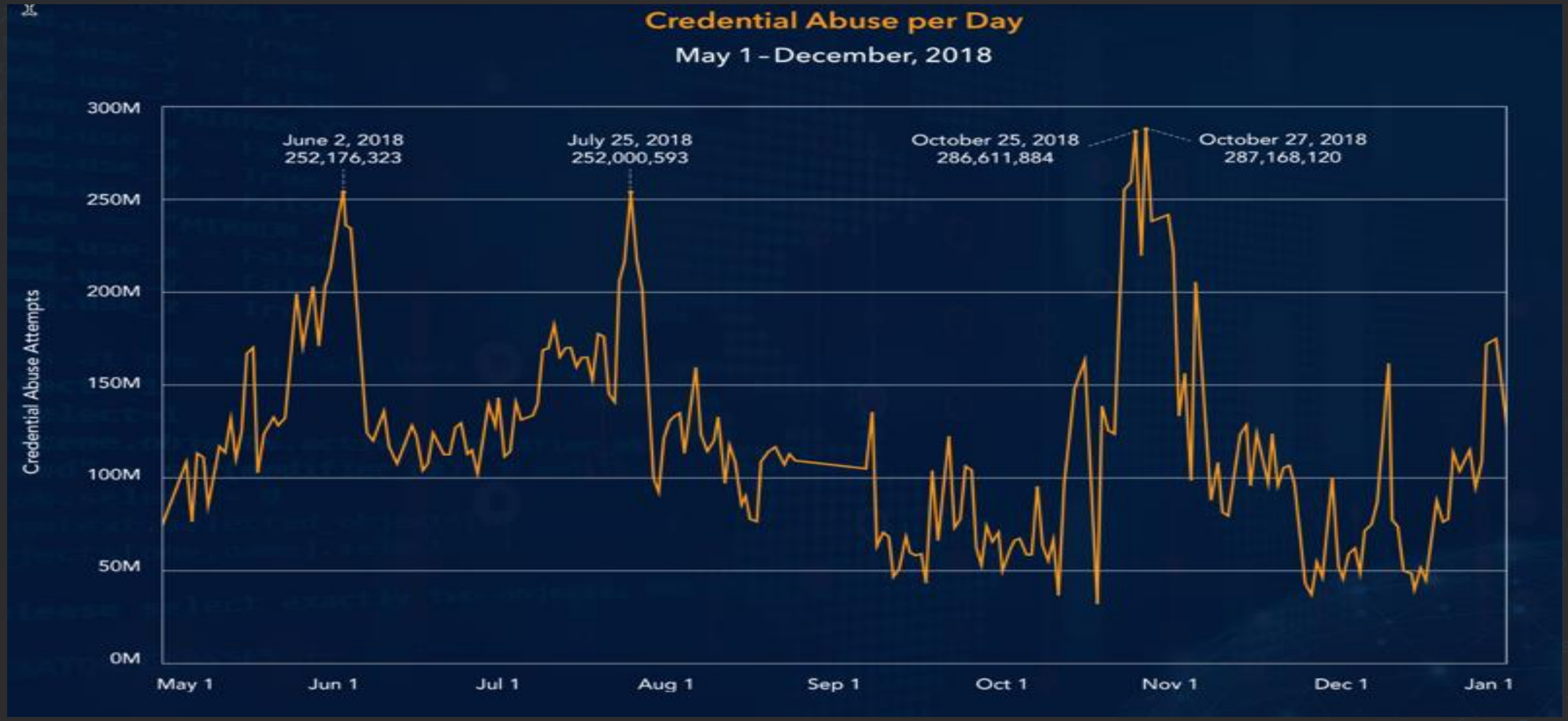


为什么安全防护如此困难？

一切都在变化，超越了您的响应速度

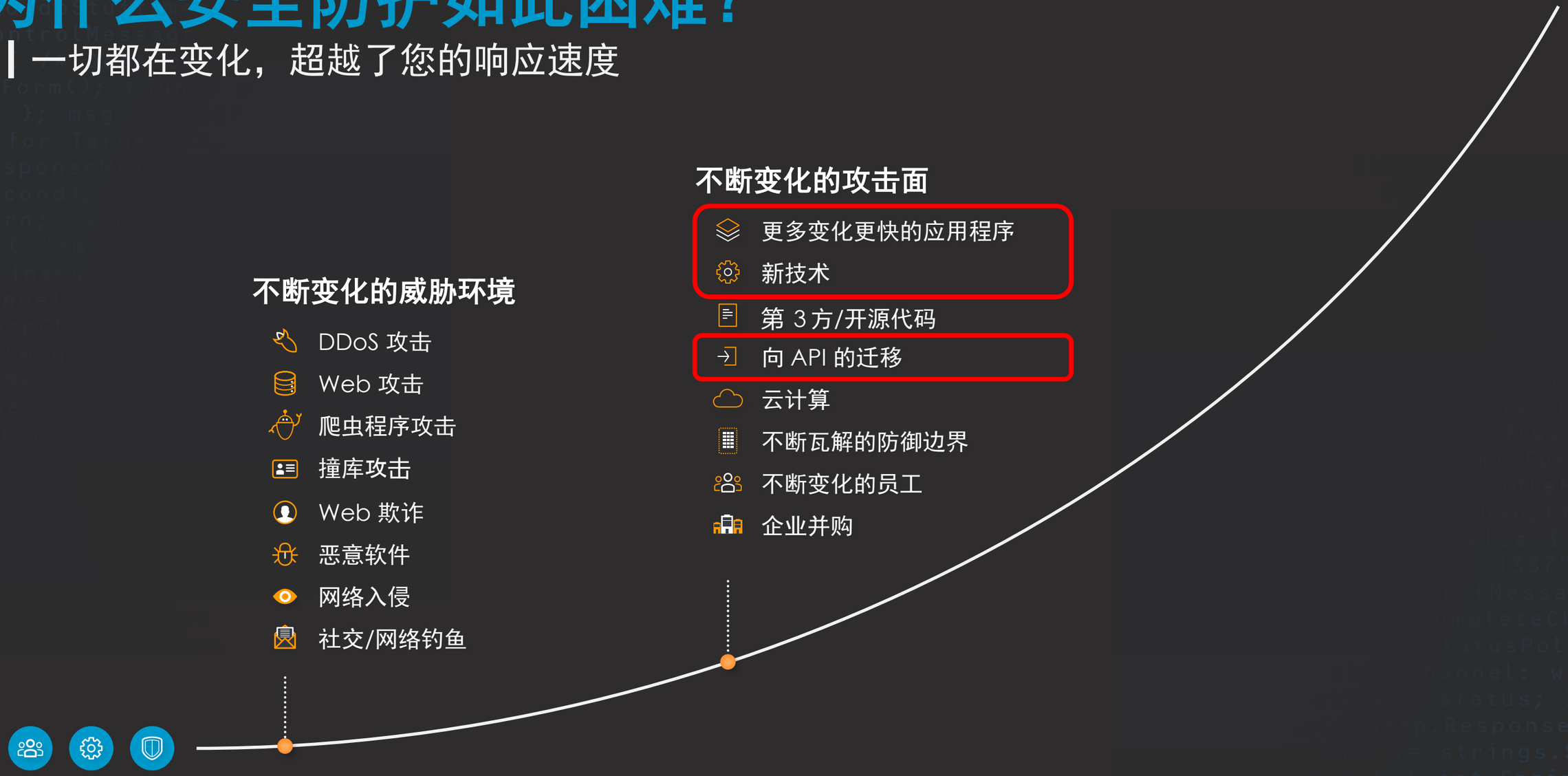
撞库攻击 - 每日攻击数

2018 年 5 月 - 12 月



为什么安全防护如此困难？

一切都在变化，超越了您的响应速度

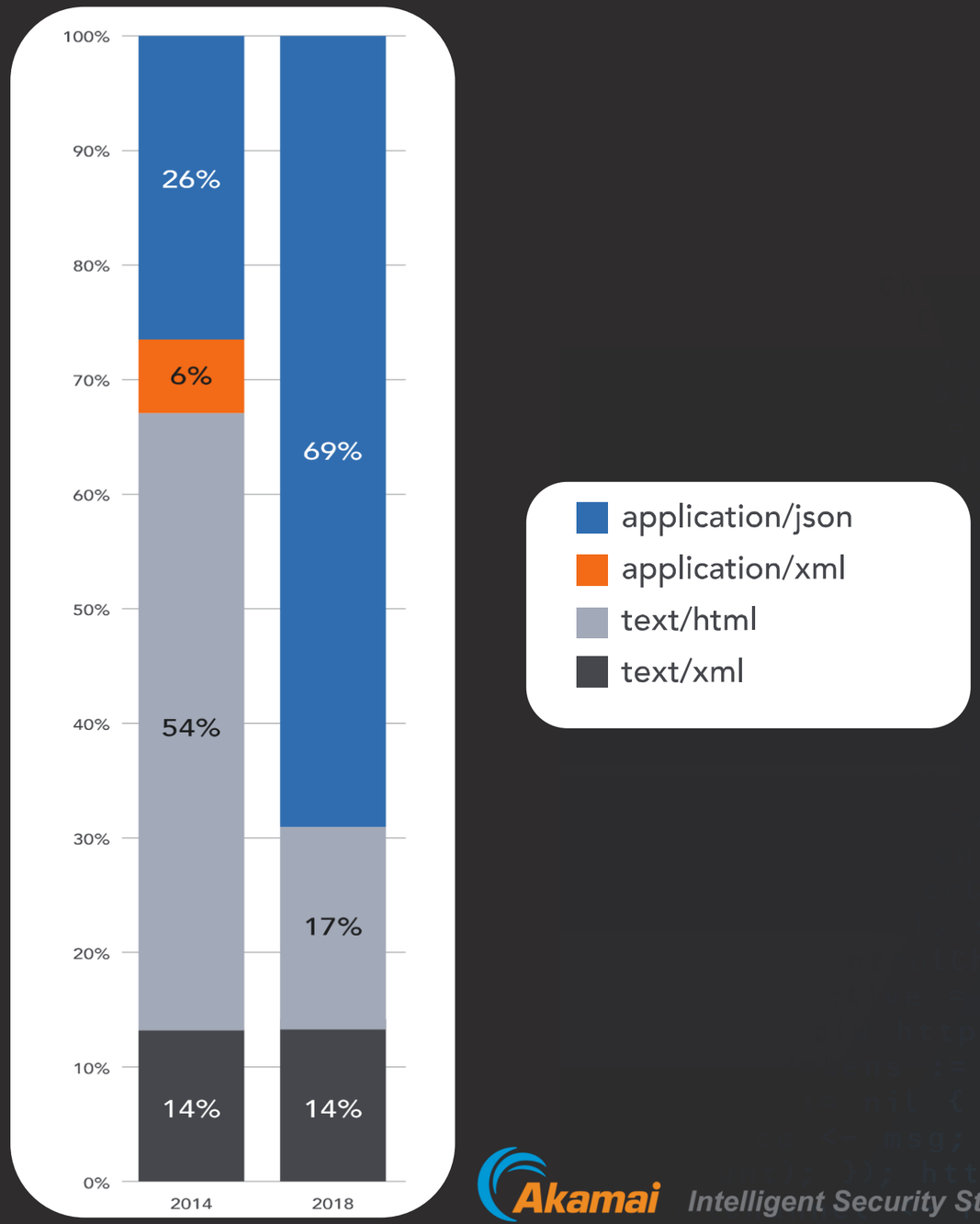


API 流量的崛起

按内容类型

巨大变化

- Web 流量现在只有 17%
- JSON 流量几乎翻了三倍
- XML 流量消失



为什么安全防护如此困难？

一切都在变化，超越了您的响应速度

不断变化的威胁环境

- DDoS 攻击
- Web 攻击
- 爬虫程序攻击
- 撞库攻击
- Web 欺诈
- 恶意软件
- 网络入侵
- 社交/网络钓鱼

不断变化的攻击面

- 更多变化更快的应用程序
- 新技术
- 第 3 方/开源代码
- 向 API 的迁移
- 云计算
- 不断瓦解的防御边界
- 不断变化的员工
- 企业并购

行业大趋势

- 数字化转型
- 移动设备采用
- 云采用
- 物联网
- 法规合规性

这对您意味着什么

对您的安全态势带来的挑战

风险增加

网络攻击的可能性和业务影响更高，而对您的响应能力的信心比以往任何时候都更低

- 无法紧跟不断变化的威胁形势
- 无法掌控全局，导致资产不受保护
- 攻击对应用程序和 IT 资产的潜在影响不断加剧

高复杂性

您负责保护的资产的快速持续变化会降低您的保护能力

- 不断扩张但理解不够到位的攻击面
- 应用程序位于多个位置，安全态势不一致
- 没有充分了解正在发生的一切

更低的敏捷性

安全组织响应业务合作伙伴需求的能力正在下降

- 无法紧跟您支持的业务的发展步伐
- 不断被动应对；没有战略意识

安全技能不足

为什么您无法应对这些挑战

150 万

Frost & Sullivan 估计的到 2020 年时的安全人力短缺

资料来源：Frost and Sullivan 研究

25%

的安全领导者将缺乏训练有素的人员视为他们面临的最大阻碍。

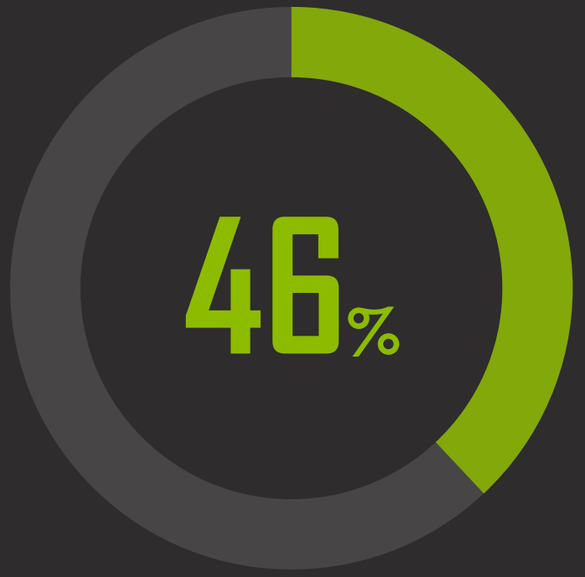
资料来源：《Cisco 2017 年度安全报告》

40%

的安全领导者将大部分时间都用在关键威胁上

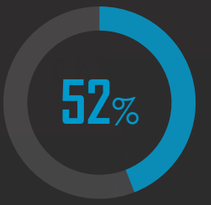
资料来源：Dark Reading《与网络攻击、数据泄露有关的网络安全人员短缺》

少于一半
的领导者具有信心



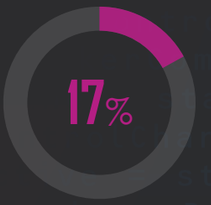
针对他们的团队处理简单网络事件以外的任何状况的能力

最大的技能不足



理解业务的能力

专业技能



沟通技巧

资料来源：数据科学中心

新模式

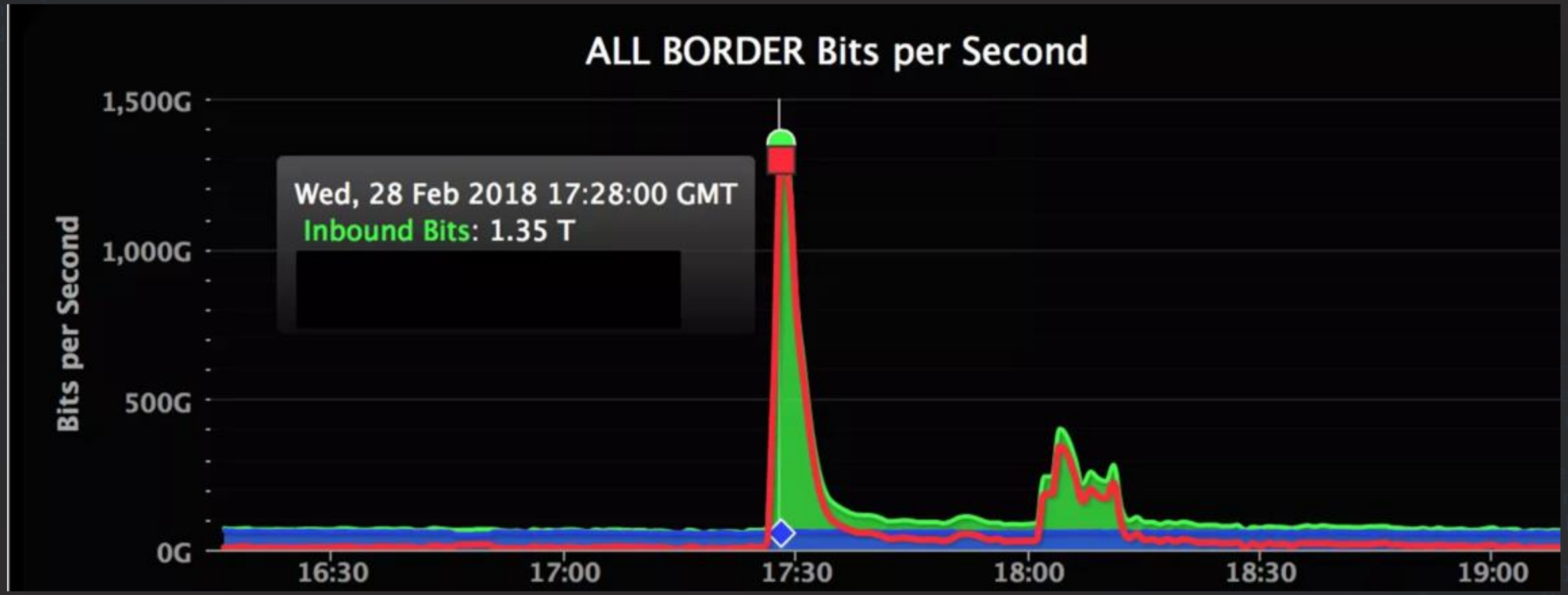
边缘为安全性提供了什么

战略平台

覆盖您的应用程序、基础设施和人员，并在全球范围内实施一致的安全策略

DDOS 攻击在持续增长

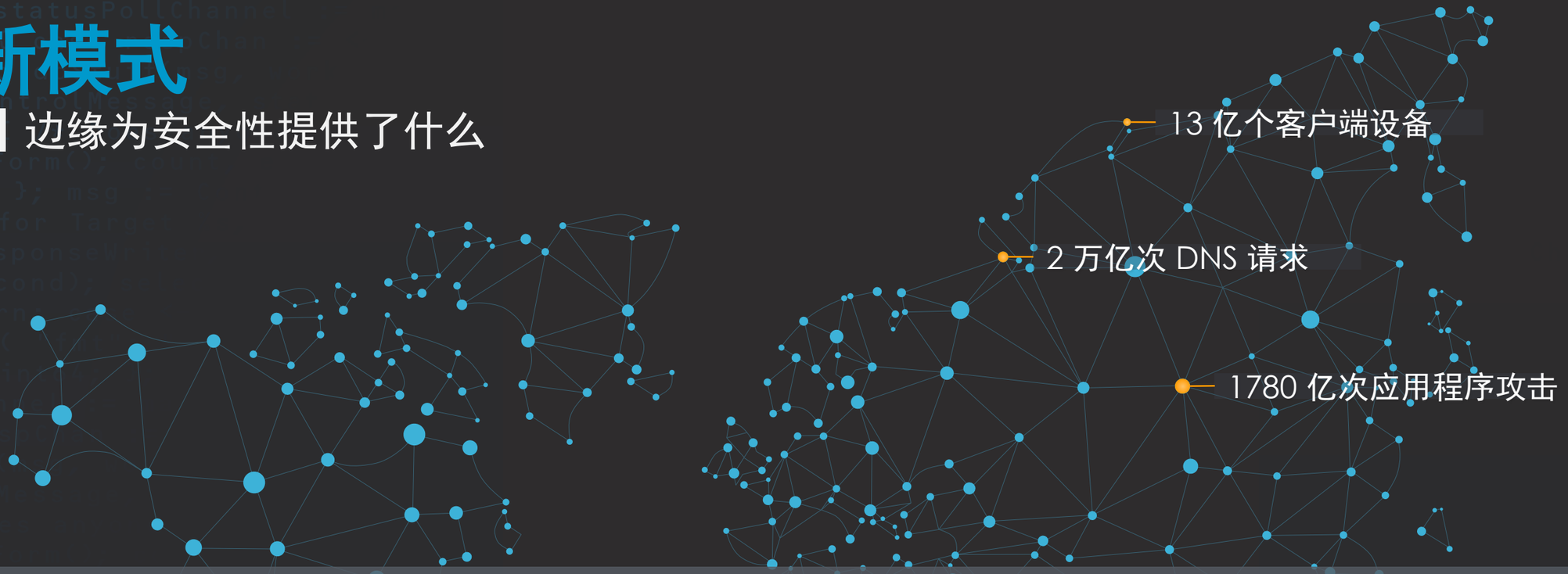
2018 年 3 月 - 1.35TB



https://github.blog/2018-03-01-ddos-incident-report/

新模式

边缘为安全性提供了什么

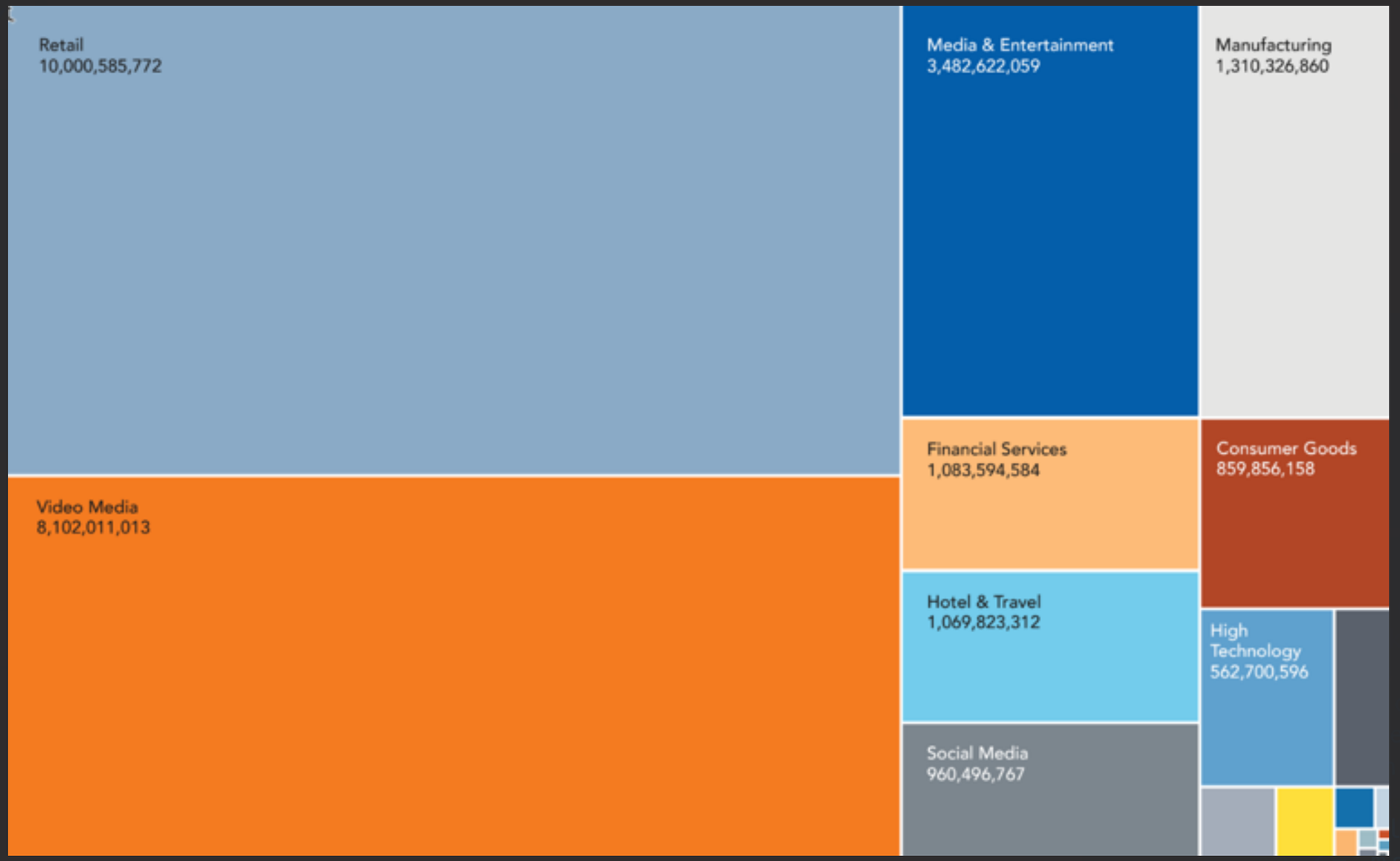


掌握攻击动向

每天可以监控数十亿次攻击，随时了解最新的威胁
（让您无需操心此类事务）

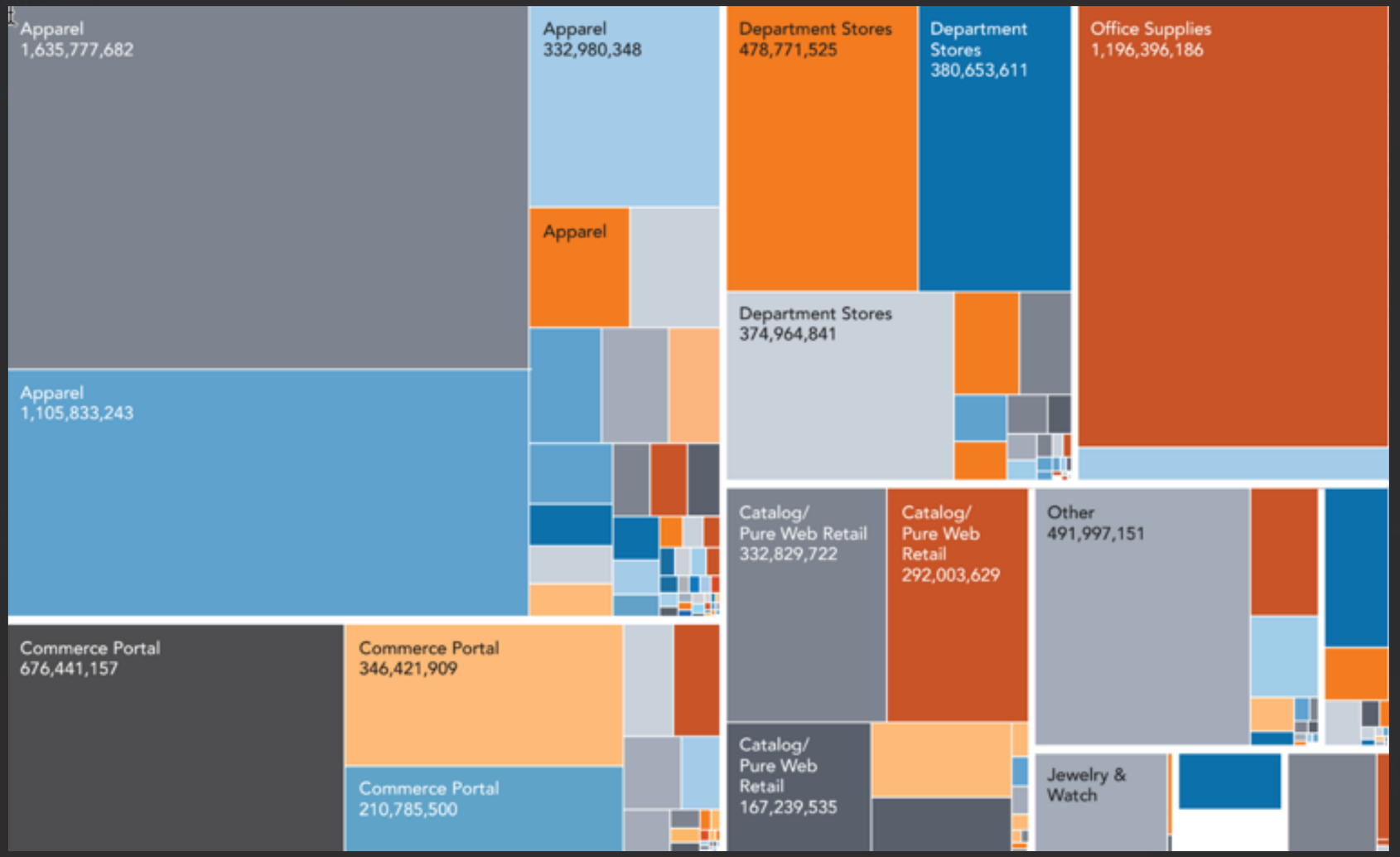
撞库攻击 - 按垂直行业

2018 年 5 月 - 12 月



撞库攻击 - 零售企业（按类型）

2018 年 5 月 - 12 月



撞库攻击 - 攻击来源

排名前 5 的国家/地区（2018 年 5 月至 12 月）

新模式

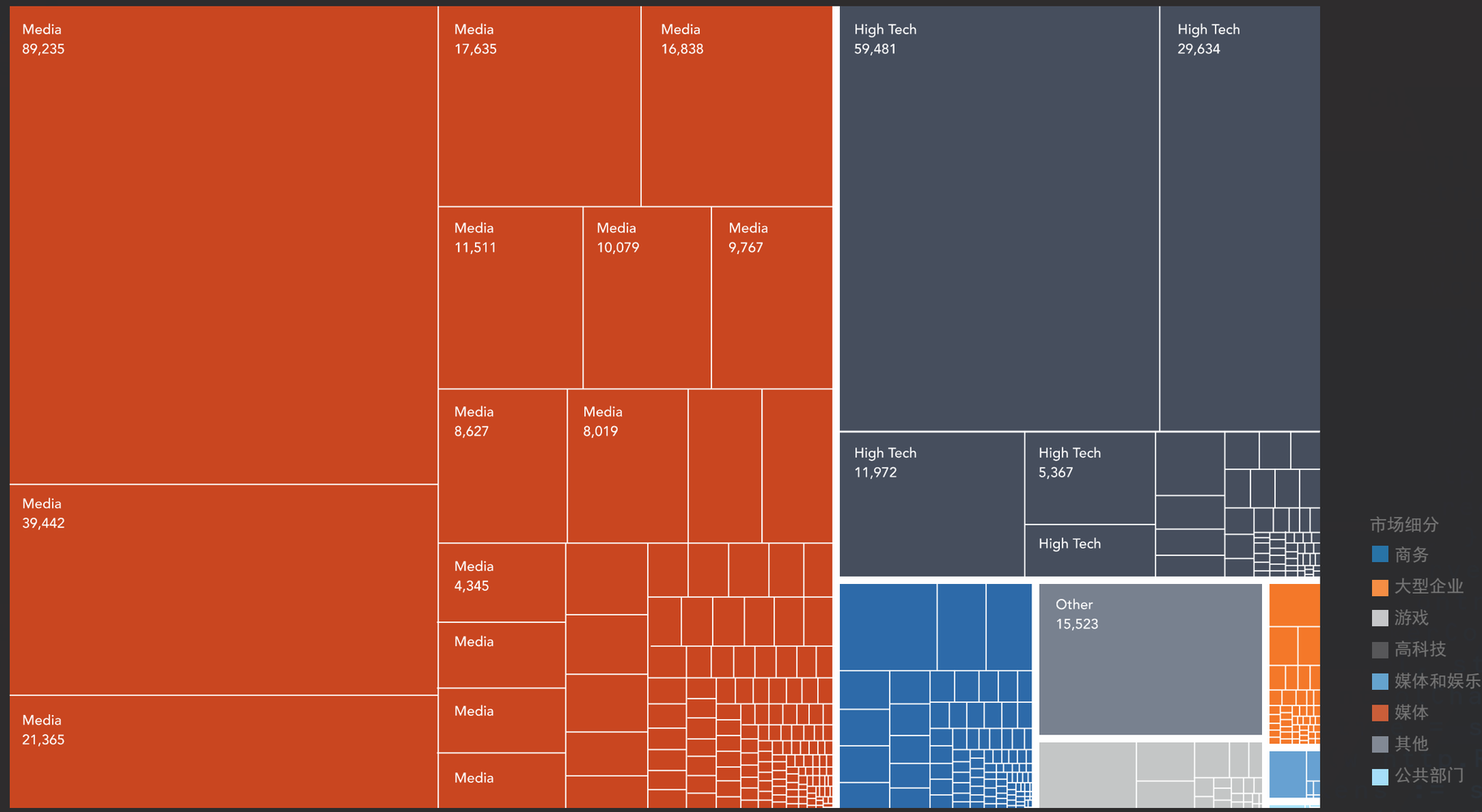
边缘为安全性提供了什么

适应业务

在办公室和数据中心、路上或云中保护您的应用程序、基础设施和人员

API 命中垂直行业与企业

（数百万次命中）



API 流量

按用户代理

TYPE	UA	
Browser	Chrome	13%
	Mobile Safari	8%
	Firefox	2%
	InternetExplorer	2%
	Edge	1%
	Safari	1%
	IE Mobile	0%
Non Browser	Other	66%
	CFNetwork	3%
	Apache HttpClient	2%

AKAMAI 边缘安全

从边缘保护您的业务

应用程序和 API

在数据中心或公共云中保护任意位置部署的面向互联网的应用程序和 API

- DDoS 防护
- Web 应用程序防火墙
- Client reputation
- API 管理
- DNS

撞库攻击

保护客户帐户防御爬虫程序攻击，并减少与欺诈相关的财务损失

- 爬虫程序管理
- 撞库攻击
- 身份管理

零信任

控制企业应用程序访问并保护用户抵御定向威胁

- 安全应用程序访问
- Web 应用程序防火墙
- 恶意软件预防

AKAMAI 边缘安全

安全与性能兼顾

应用程序和 API

- DDoS 防护
- Web 应用程序防火墙
- Client reputation
- API 管理
- DNS

撞库攻击

- 爬虫程序管理
- 撞库攻击
- 身份管理

零信任

- 安全应用程序访问
- Web 应用程序防火墙
- 恶意软件预防

应用程序加速

AKAMAI 智能边缘安全

基于边缘的安全性的市场领导者

保护应用程序和 API	阻止撞库攻击	迁移到零信任
DDoS 和 WAF **领导者**	爬虫程序管理 **领导者**	Zero Trust eXtended 生态系统 **表现优异者**
FORRESTER® Gartner	FORRESTER® FROST & SULLIVAN	FORRESTER®

*长期以来，Akamai 一直拥有**强大、广泛的边缘安全产品和服务**.....*

- IDC

边缘安全：新模式

边缘应成为您的防御边界

战略平台

覆盖您的应用程序、基础设施和人员，并在全球范围内实施一致的安全策略

谢谢

Intelligent Security Starts at the Edge