ONE ASP RASP

企业如何构建安全防护壁垒

孙政豪

目录

国内安全事件

事件回顾

2016年1月4日，汇丰银行遭受不明流量攻击，系统崩溃，服务中断两天;1月29日，汇丰银行再次遭受DDoS攻击，服务再次陷入瘫痪，业务损失惨重。由此可以窥见，2016年DDoS攻击将再度猖獗。

作为对安全性和稳定性都要求极高的金融企业，汇丰银行自身的安全防御系统应该是行业较高标准的，但形式日趋多样的DDoS攻击已然攻破防线，给所有有被攻击风险的企业敲响了警钟。在信息化高速发展的现在，任何业务系统的被攻击、中断都是企业“不能承受之重”。游戏企业遭受攻击，玩家游戏中断，用户体验极差;电商企业遭受攻击，用户无法购物，必然会失去继续使用该网站的兴趣，企业面临失去大量用户的风险;金融企业遭受攻击，资产管理系统中断，后果难以想象。此类事例每天都在发生，及时做好网络安全防范已经刻不容缓。

一支名为China 1937CN Team的中国黑客活动组织已经对21座越南机场发动攻击，并篡改了各越南国有航空公司的官方网站。

本周五下午——7月29日——河内市的内拜机场与胡志明市的新山机场遭遇黑客攻击。

黑客破坏了机场的语音与视频系统，并开始广播指向越南及菲律宾的攻击性信息，同时宣称东越南海为中国统治下的领土。

广播的音频信息为英文版本，目前越南媒体已经获得了一份语音副本。

21座越南机场遭遇计算机系统故障

当天晚些时候，官员进一步报告称机场的计算机系统开始出现故障，当天下午21点左右越南各地的机场被迫转而以手动方式办理乘机手续。

一周大事件|被骗学费离世,谁害死了"徐玉玉们"

网易新闻 2016年08月26日 10:11

8月21日,山东临沂的准大一新生徐玉玉,被一通诈骗电话骗走家人辛苦一年攒下的9900元学费,两天后遗憾离世,再度引发人们对电信诈骗的关注。19... 百度快照

国际安全事件

这一次，俄罗斯黑客成功的进行了一场大规模的数据泄露事故。在此次网络攻击中，黑客盗取了2.723亿个帐号，以俄罗斯最受欢迎的电子邮件服务Mail.ru用户为主，此外还有Gmail地址、雅虎以及微软电邮Hotmail用户。路透社称，数以亿计的数据目前正在“俄罗斯的地下黑市”出售。

超3200万Twitter账户密码泄露

来自Leaked Source的消息，上周，俄罗斯社交网站VK.com遭入侵，1.71亿用户帐号信息泄露，泄露这些信息的黑客名为Tesso88。而Twitter这次泄露的数据信息同样来自此人：超过3200万Twitter用户的登录信息正在暗网黑市出售，价格为10比特币(超过人民币38000元)。

全球DDoS峰值2016上半年破纪录达579Gbps

2016.07.21 10:50:00　来源: 199IT　作者:199IT　(0 条评论)

由信息安全公司Arbor Network统计的信息安全报告，2016年上半年期间全球DDoS峰值记录突破了新高－突破了之前的500Gbps（2015年底）达到了 579Gbps。

报告还指出，尽管此期间DDoS攻击的峰值速率突破了新高，但在此期间每起攻击的平均值下降至986Mbps，这意味着部署DDoS攻击 缓速硬件设施的企业都能抵御大部分攻击。

安全的现状

- 超过80%的攻击发生在应用层
- 多样化的攻击越来越难以防御
- Web系统开发商在安全领域投入少

常见的网络层DOS攻击方式

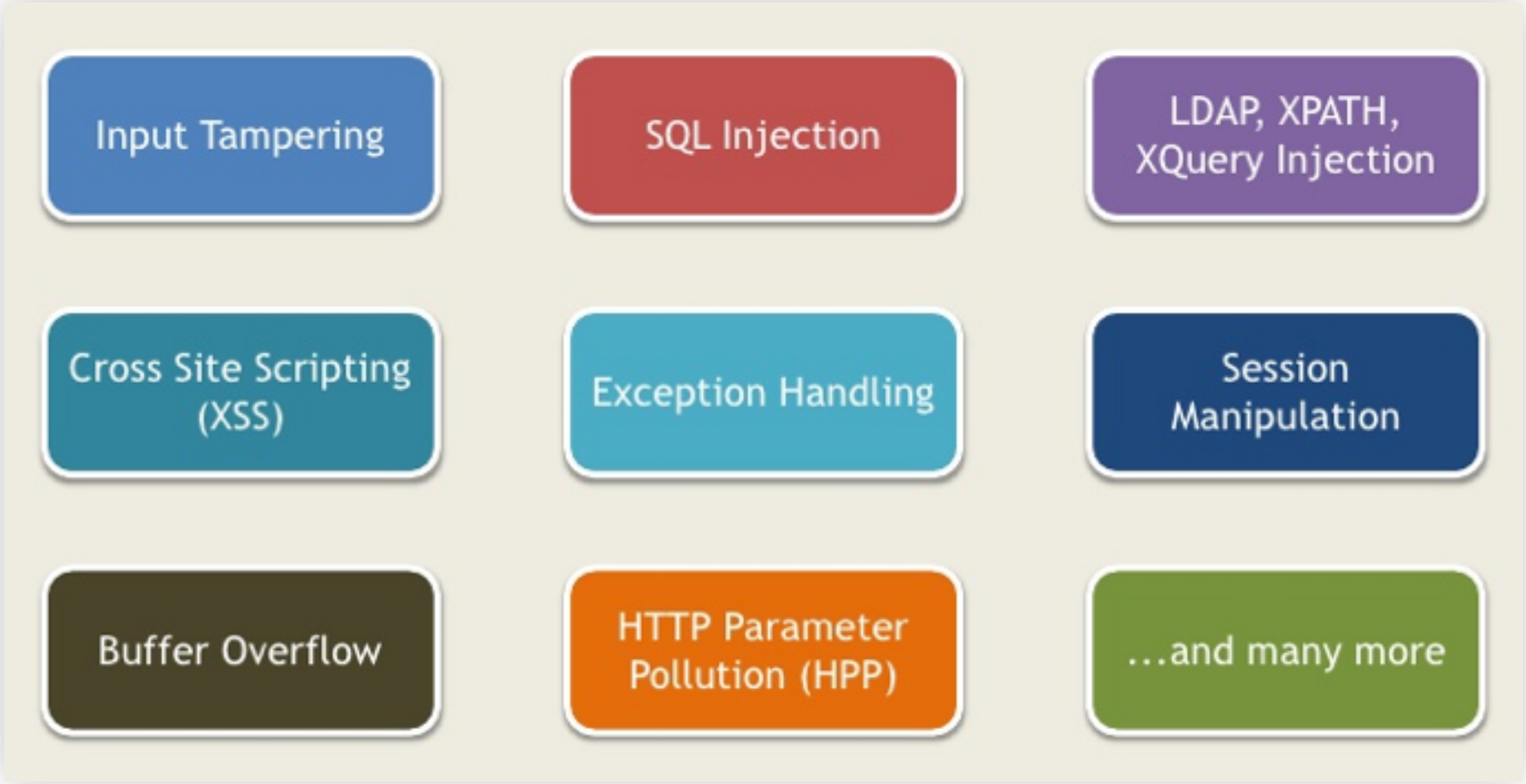
- Ping of Death
- Teardrop
- Flood
- Land
- Smurf
- 分布式拒绝服务攻击

网络空间是一个非常危险的领域 ….

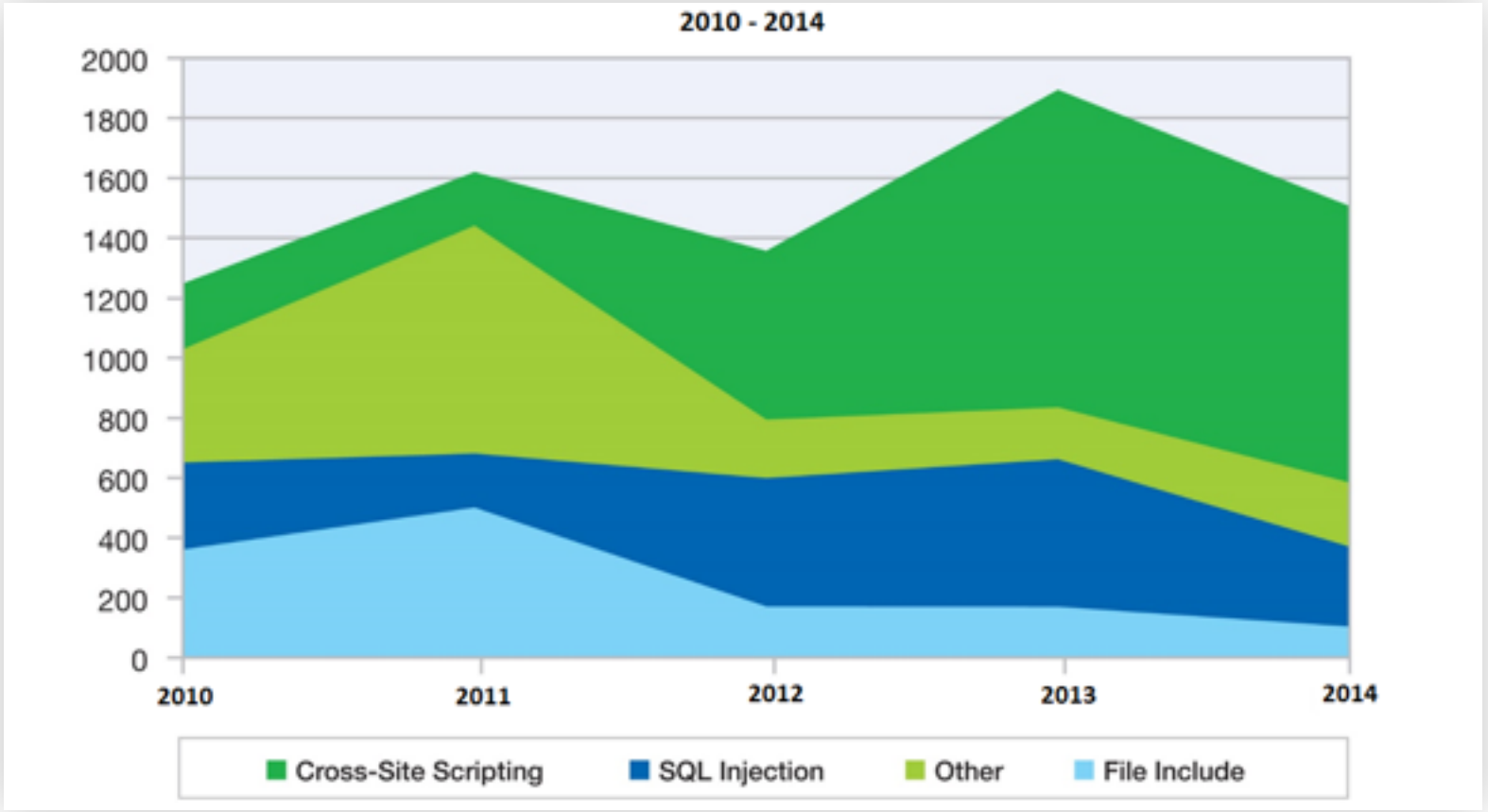
常见威胁分析

- Web常用的攻击方式
- OWASP Top 10

Web常用的攻击方式


Input Tampering
SQL Injection
LDAP, XPATH, XQuery Injection
Cross Site Scripting (XSS)
Exception Handling
Session Manipulation
Buffer Overflow
HTTP Parameter Pollution (HPP)
...and many more

主流的Web攻击方法



资料来源：IBM X-Force®研究与发展

OWASP Top 10

OWASP Top 10 – 2010 （旧版）	OWASP Top 10 – 2013 （新版）
A1 – 注入	*A1* – 注入
A3 – 失效的身份认证和会话管理	*A2* – 失效的身份认证和会话管理
A2 – 跨站脚本（*XSS*）	*A3* – 跨站脚本 （*XSS*）
A4 – 不安全的直接对象引用	*A4* – 不安全的直接对象引用
A6 – 安全配置错误	*A5* – 安全配置错误
A7 – 不安全的加密存储 – 与*A9*合并成为→	*A6* – 敏感信息泄露
A8 – 没有限制*URL*访问 – 扩展成为→	*A7* – 功能级访问控制缺失
A5 – 跨站请求伪造（*CSRF*）	*A8* – 跨站请求伪造（*CSRF*）
<合并在*A6* – 安全配置错误>	*A9* – 使用含有已知漏洞的组件
A10 – 未验证的重定向和转发	*A10* – 未验证的重定向和转发

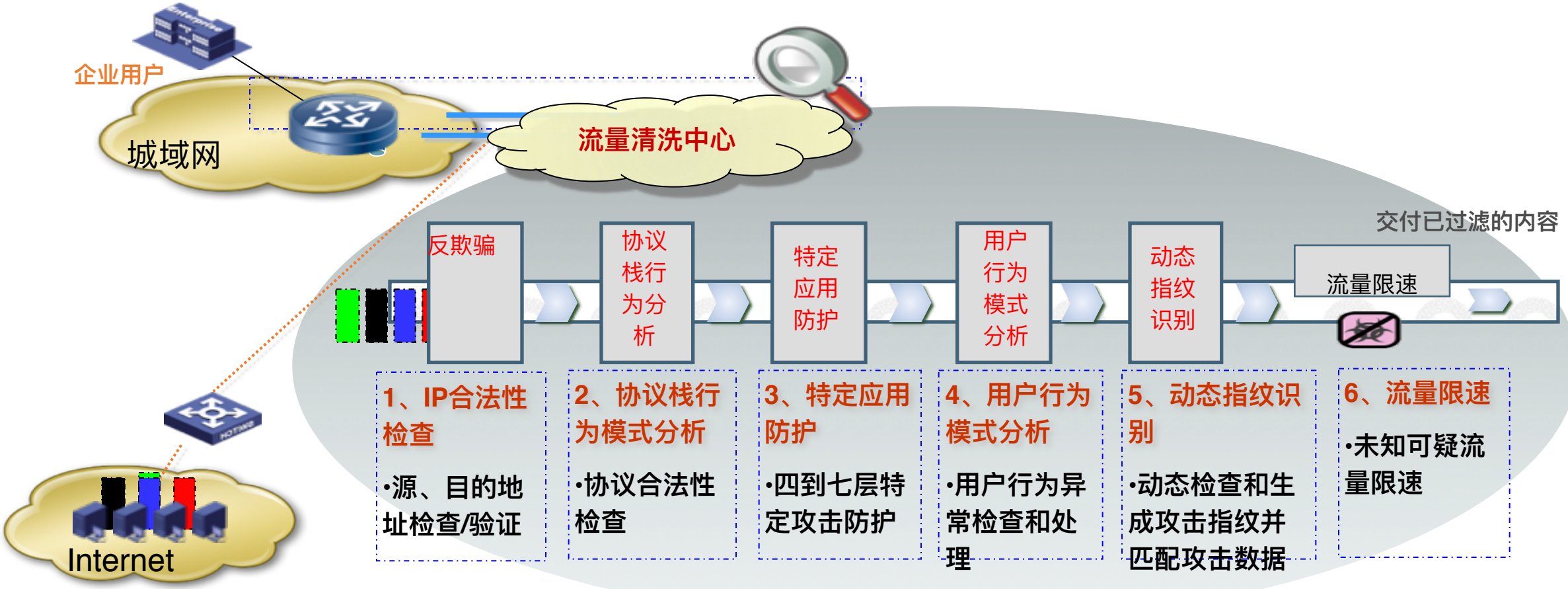
常见的防护方法

分层次防御

- 提高攻击者被检测到的概率
- 降低攻击者成功得手的几率

物理层防御	Security Guard , CCTV
网络层防御	网段，安全，防火墙，网络访问间隔控制，IPS/IDS
主机防御	OS hardening ， 认证，补丁管理，基于主机的 AV ， 基于主机的 IDS ， 基于主机的 FW
应用程序防御	Application hardening , SSDLC , AST(SAST , DAST , IAST), WAF
数据和资源	ACLs , encryption , EFS

流量清洗工作原理


企业用户
城域网
流量清洗中心
交付已过滤的内容
反欺骗
协议栈行为分析
特定应用防护
用户行为模式分析
动态指纹识别
流量限速
Internet
1、IP合法性检查
•源、目的地址检查/验证
2、协议栈行为模式分析
•协议合法性检查
3、特定应用防护
•四到七层特定攻击防护
4、用户行为模式分析
•用户行为异常检查和处理
5、动态指纹识别
•动态检查和生成攻击指纹并匹配攻击数据
6、流量限速
•未知可疑流量限速

常见的防护方法

分层次防御

- 提高攻击者被检测到的概率
- 降低攻击者成功得手的几率

物理层防御	Security Guard , CCTV
网络层防御	网段，安全，防火墙，网络访问间隔控制，IPS/IDS
主机防御	OS hardening ， 认证，补丁管理，基于主机的 AV ， 基于主机的 IDS ， 基于主机的 FW
应用程序防御	Application hardening , SSDLC , AST(SAST , DAST , IAST), WAF
数据和资源	ACLs , encryption , EFS

应用层防御

- 主动防御方式：渗透测试、SSDLC、AST
- 被动防御方式：WAF、RASP
- 安全大数据：威胁情报、行为异常管理 等等

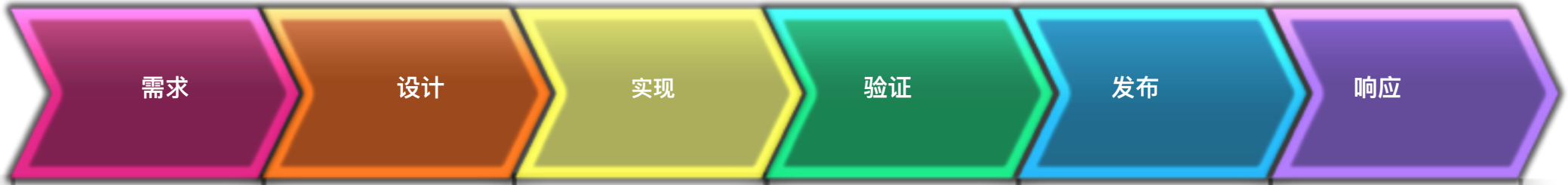
常见的防护方法

分层次防御

- 提高攻击者被检测到的概率
- 降低攻击者成功得手的几率

物理层防御	Security Guard , CCTV
网络层防御	网段，安全，防火墙，网络访问间隔控制，IPS/IDS
主机防御	OS hardening ， 认证，补丁管理，基于主机的 AV ， 基于主机的 IDS ， 基于主机的 FW
应用程序防御	Application hardening , SSDLC , AST(SAST , DAST , IAST), WAF
数据和资源	ACLs , encryption , EFS

安全软件开发生命周期-SSDLC



- **产品研发初期**
- 安全顾问规划
- 规划安全里程碑
- 安全元素集成入产品

- **设计**
- 设计安全架构和指导方案。
- 形成安全且有效的规范完档

- **漏洞模型**

- **标准、检验、工具**

- 遵从安全编码规范
- 使用安全扫描工具(fuzzing tools, static-analysis tools, etc)

- **安全性推动**
- 代码reviews
- 安全性测试
- 主流漏洞监测
- 达到预期准则

- **安全性把控**
- 安全团队的检测
- 完整的测试验证
- 遵守安全准则

- **RTM 和 部署**

- **安全响应**
- 规范反馈响应机制
- 实时处理反馈
- 反思

安全领域的指导

人才少见

缺乏安全且有效的流程

指导文档

研发团队往往很少

考虑安全因素

Web应用防火墙

Web应用防火墙（WAF）是部署在Web服务器的入口

检测所有进入服务器的报文通过正则表达式的方式匹配报文的特征字段，来判断是否为攻击。

降低数据泄露风险

用精炼的规则对攻击实施过滤，加上HTTP协议合规检查、状态码过滤等机制，降低数据泄露风险。

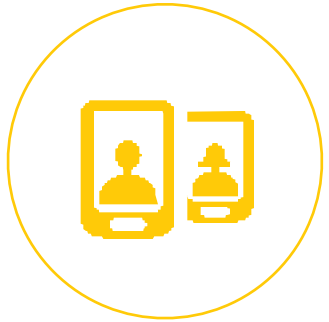
支持Web服务可用性

集成DDoS防护功能，与SQL注入防护等功能一起使用，提供多层次攻击过滤，支撑Web服务可用性。

控制恶意访问

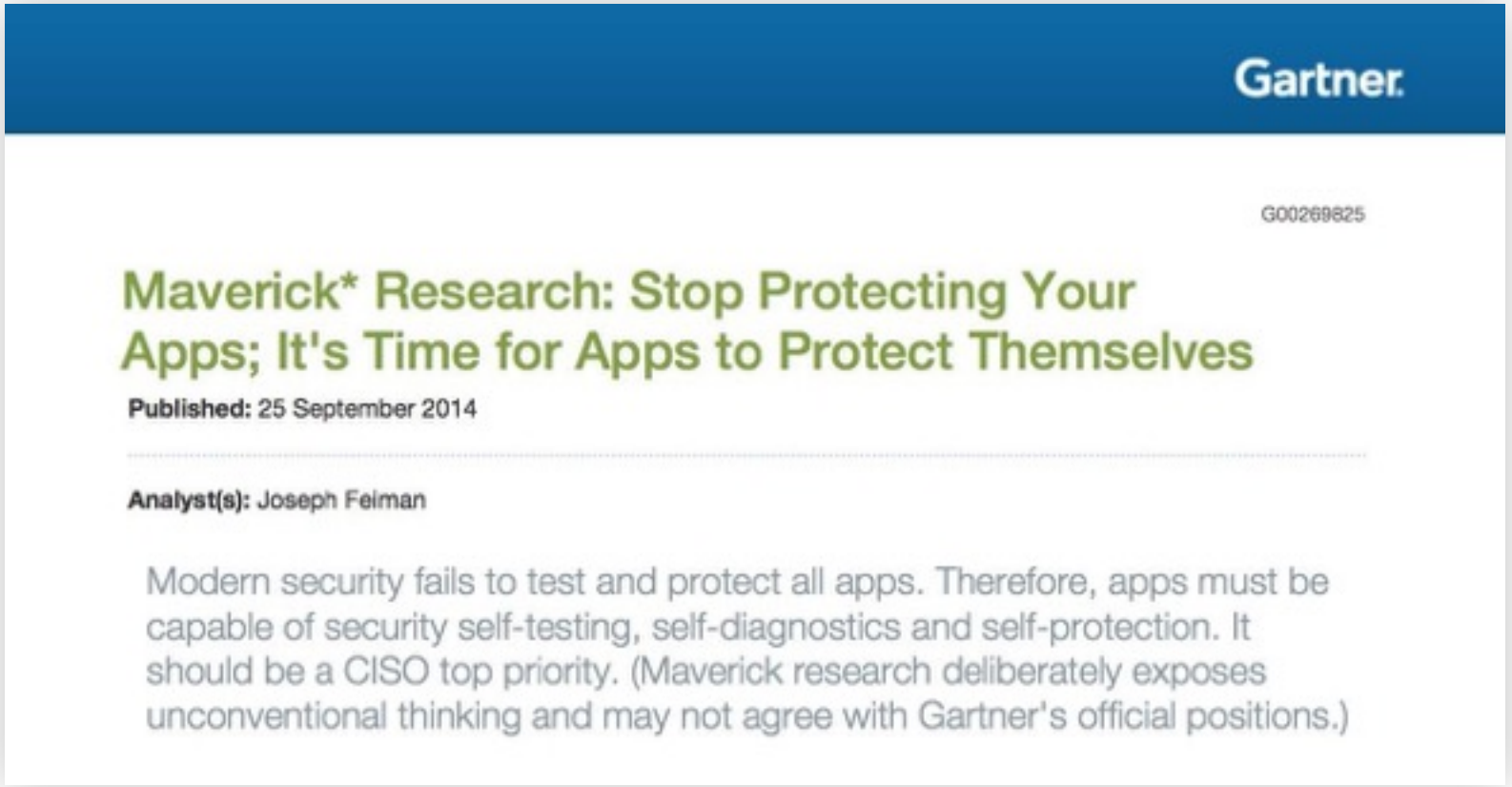
支持多种Web访问控制，包括HTTP访问控制、自动化攻击工具识别、控制非法文件上传和下载、阻止盗链和爬虫等。

保护Web客户端



提供CSRF防护、XSS防护、Cookie签名和加密等安全策略，保护Web客户端。

RASP, 运行时应用自我防护



Gartner

G00269825

Maverick* Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves

Published: 25 September 2014

Analyst(s): Joseph Feiman

Modern security fails to test and protect all apps. Therefore, apps must be capable of security self-testing, self-diagnostics and self-protection. It should be a CISO top priority. (Maverick research deliberately exposes unconventional thinking and may not agree with Gartner's official positions.)

实时应用自我保护技术（Runtime Application Self－Protection）也称RASP技术，是2014年9月Gartner的调研员Feiman提出的一种全新概念。

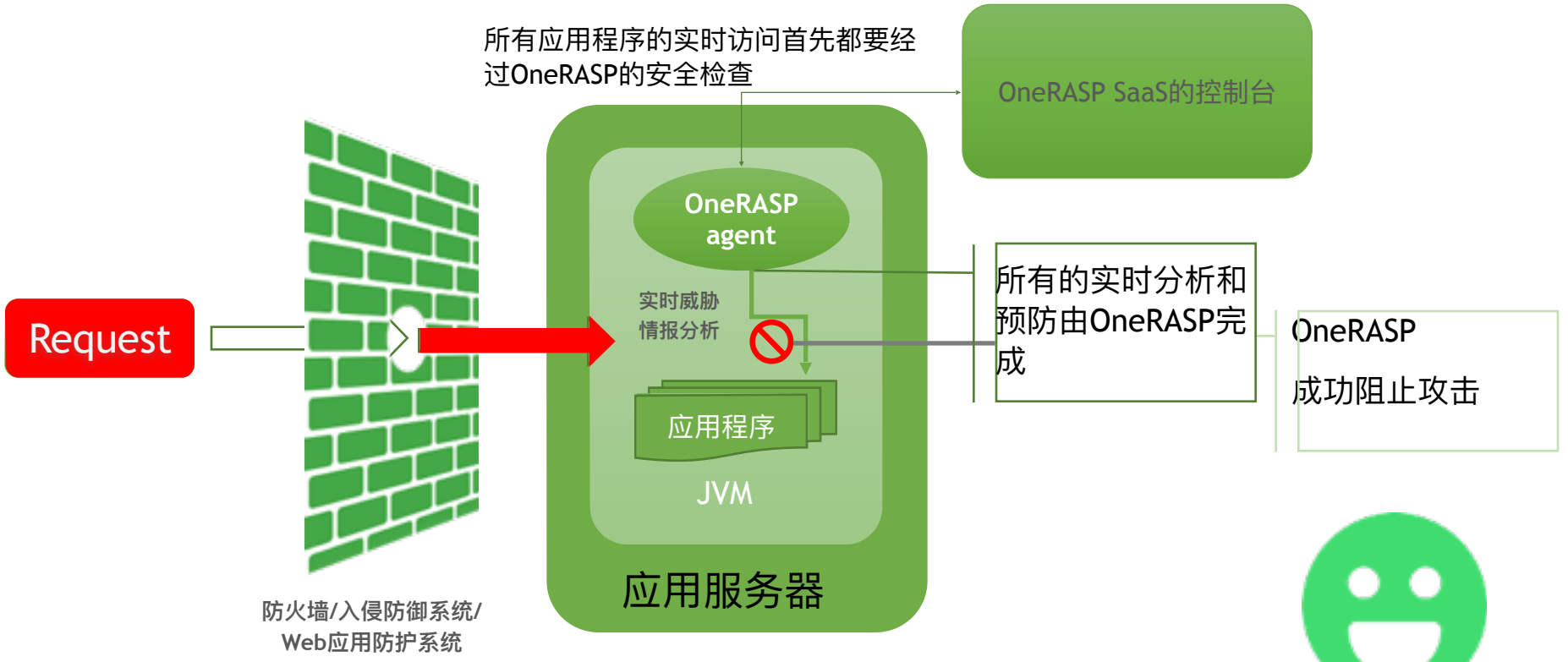
他指出，网络的边界逐渐在消失，同时诸如WAF这类的“边界保护”技术也无法深入应用内部，对应用的逻辑数据流理解不全面，由此带来的误杀率高的现象时有发生。

为什么需要RASP技术

- 程序完成的太久远，找不到源代码
- 漏洞数量太多
- 缺少安全专家去推动SSDLC
- 开发团队缺乏安全经验
- 第三方供应商的漏洞修复周期长
- 系统中存在未知的漏洞

所以，你需要使用RASP产品打**虚拟补丁**，来保护你的应用程序

OneRASP请求实例图



它像一剂疫苗注入到应用中，与应用一起运行，对外提供服务

结合应用的逻辑和数据流，在运行时对访问应用的代码进行检测

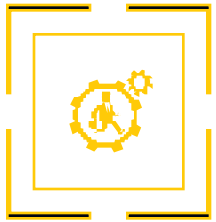
对于已知漏洞，相当于为其打了虚拟补丁，起到补偿控制后的作用

对互商行业的建议

树立安全防护意识

这个世界上一共有两种公司：一种被「黑」过，另一种，不知道自己被「黑」过。

安全防护工作，不能存在任何侥幸心理。



谨慎选择安全防护方案

市面上的安全防护方案鱼龙混杂，很大部分已经完全不适应如今的网络威胁形势，两点建议：

1. 不要试图通过让系统变复杂来换取安全，越复杂越容易暴漏缺陷。

2. 充分考察解决方案的合理性，预防因方案漏洞引入了新的威胁。

没有一劳永逸的方案

黑客攻击手段越来越先进，安全防护方案不可能是一成不变的，

持续关注安全防护的发展方向，时刻做最有效的调整。

谢谢！