RASP技术在中国的落地与实践

田强
云锁产品总监

目录

RASP的概念

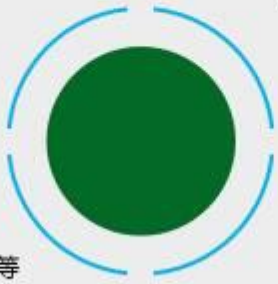
企业安全面临的风险和挑战

业务环境安全问题

应用漏洞
系统漏洞

模糊的网络边界

云环境部署，公有云、私有云、混合云
业务弹性增长



攻击手段多样化

SQL注入、跨站、请求伪造等
Webshell

传统解决方案云上效果不佳

传统设备无法部署
维护成本较高

RASP的概念

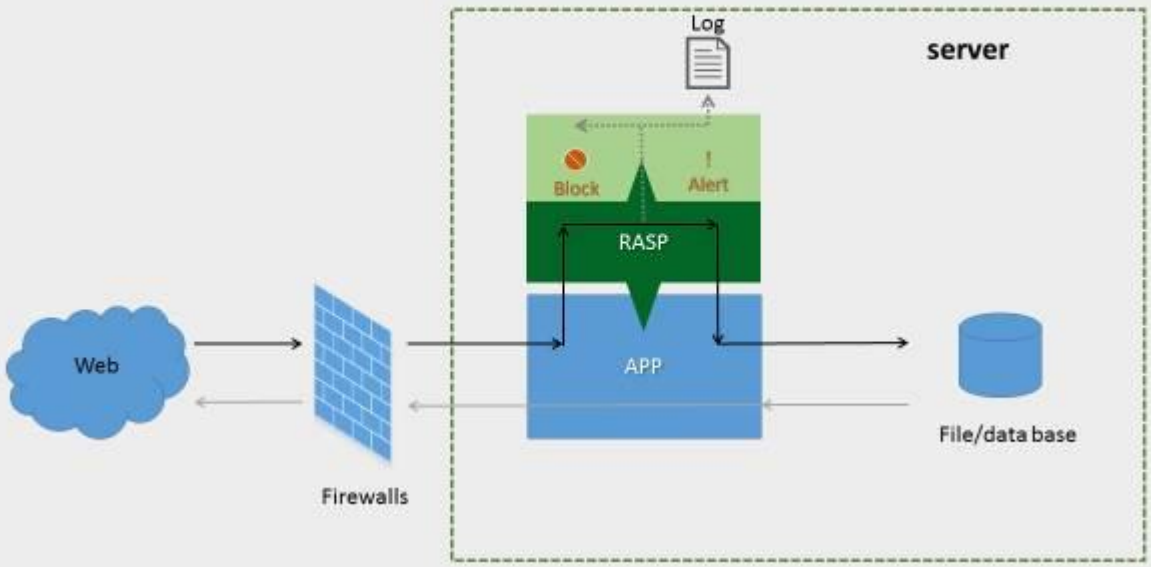
什么是RASP？

RASP（Runtime Application Self-Protection）实时应用自我保护

是一种新型应用安全保护技术，在2014年Gartner安全报告中首次被提出，它内置到应用程序中和应用程序融为一体，可以实时检测和阻断安全攻击，使应用程序具备自我保护能力，当应用程序遇到特定漏洞和攻击时不需要人工干预就可以自动重新配置应对新的攻击。

RASP 不同于传统的安全技术仅在网络周边或者终端设备上进行保护，它能够让应用程序具备自我保护能力。而实时性是 RASP 非常重要的特点，因为不仅可以分析应用程序的行为也可以分析程序的上下文；而且持续不断的分析可以在发现有攻击行为能立刻进行响应和处理。

RASP的工作原理



RASP的工作原理

RASP 与 WAF的对比

RASP	WAF
极高的覆盖度和兼容多种协议	Http协议
保护更全面	仅监控用户输入
误报率低	误报率较高
风险点定位更快速、更准确	无法快速、准确的定位风险点
不依赖网络边界	依赖网络边界
维护及学习成本低	维护及学习成本较高

RASP的工作原理

RASP 的作用

- **监视运行环境**

  监视运行环境的安全，如JVM、.NET公共运行库、容器、动态链接库、文件系统等

- **应用深度分析**

  深入应用的逻辑、配置、数据、事件流，联系上下文分析并阻止如SQL注入、跨站脚本、请求伪造等攻击和防护Webshell、反序列化、Struts 2等漏洞

- **应用过程安全检测**

  根据上下文洞察应用逻辑和数据流的异常

RASP的工作原理

RASP 的保护模式

RASP有两种模式，分别是检测模式和保护模式。检测模式在检测到安全攻击时只是记录下来并发送警告给用户，保护模式不仅能够检测攻击同时能够实时拦截潜在的安全攻击。

RASP的保护行为有以下几种方式：

- 终止用户会话
- 停止用户程序（不影响服务器上其他程序）
- 发送警报给专门的安全人员
- 发送警告给用户

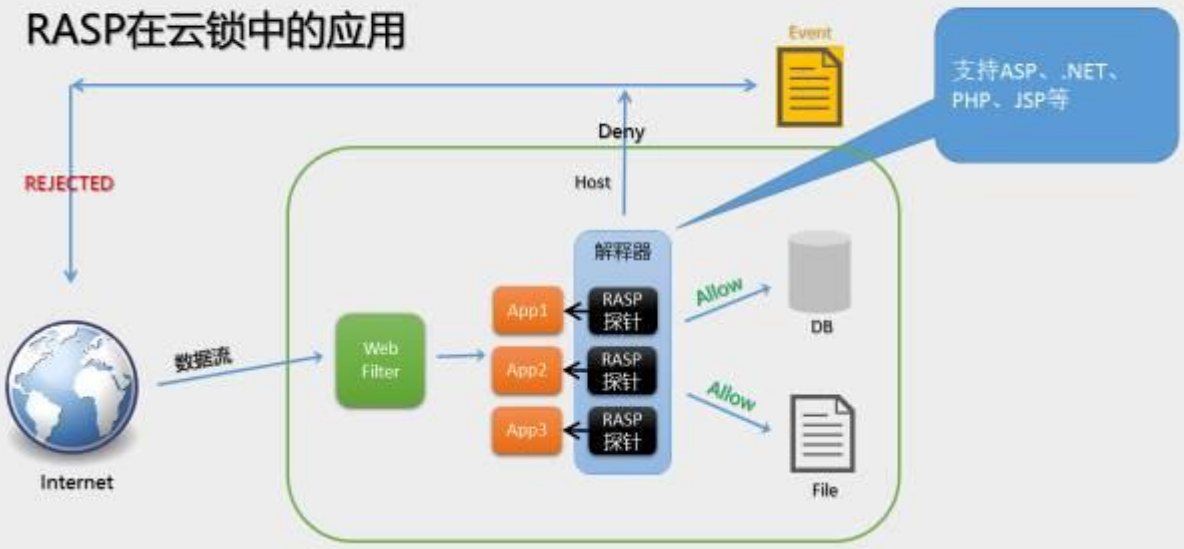
RASP的应用

RASP在国内外的应用

- Fortscale（https://fortscale.com）
- Waratek（https://www.waratek.com）
- 云锁（http://www.yunsuo.com.cn）
- ……

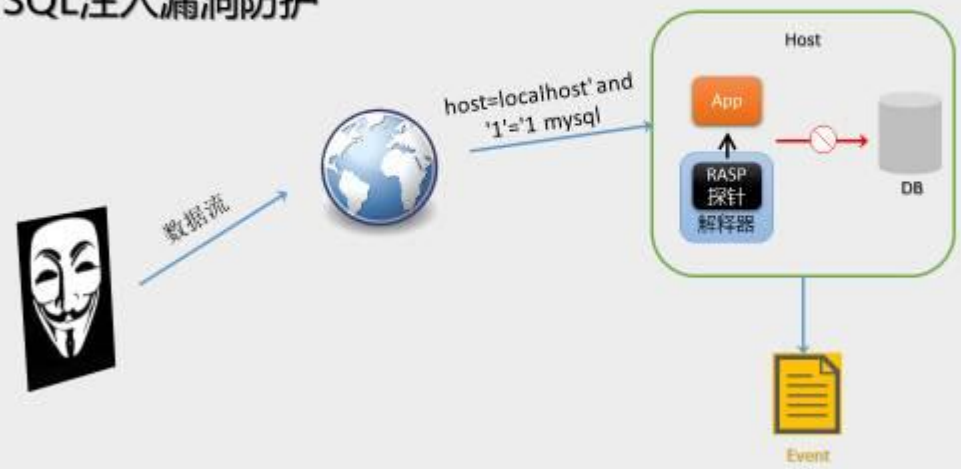
RASP的应用

RASP在云锁中的应用



RASP的应用

SQL注入漏洞防护



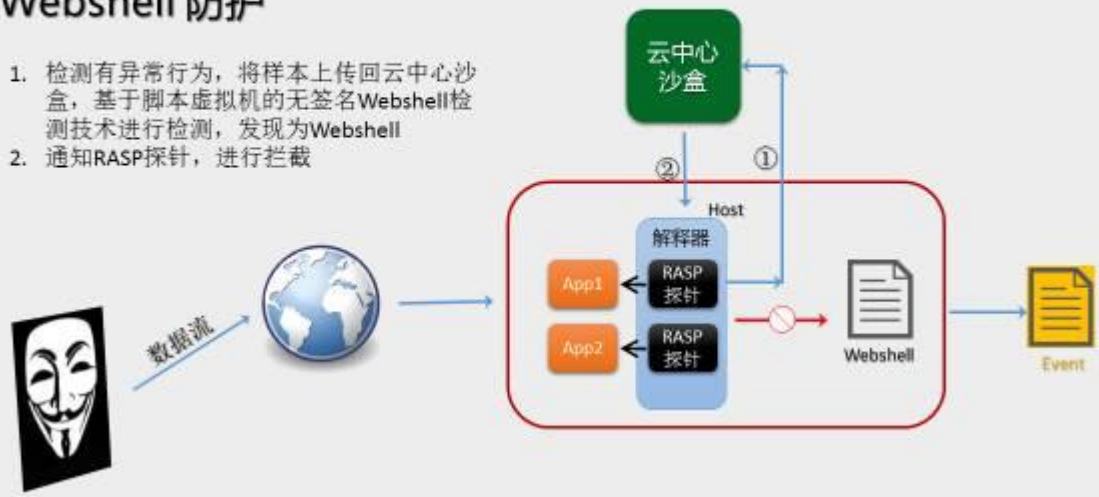
RASP的应用

SQL注入漏洞防护

RASP的应用

Webshell 防护

1. 检测有异常行为，将样本上传回云中心沙盒，基于脚本虚拟机的无签名Webshell检测技术进行检测，发现为Webshell
2. 通知RASP探针，进行拦截



RASP的应用

Webshell 防护

RASP的应用

文件上传漏洞防护

1. Web APP 创建可执行文件
2. RASP监控到创建可执行文件则进行回溯，发现为Upload行为
3. 通知文件监控驱动进行拦截
4. 文件驱动阻截该行为

RASP的应用

文件上传漏洞防护

RASP的应用

除上述几种漏洞防护外，RASP还可对其他漏洞进行防护

- Struts 2 漏洞
- 反序列化漏洞
- 任意文件读取漏洞
- 命令执行漏洞
- 文件包含漏洞
- ……

谢谢！

椒图科技 深圳总公司
地址：深圳市南山区科技南十二路18号长虹科技大厦1302室
邮编：518057
总机：0755-86638038
传真：0755-86638028
网址：www.jowto.com

椒图科技 北京分公司
地址：北京市海淀区西小口路66号中关村东升科技园北领地B-2号楼六层C601室
邮编：100192
总机：010-65014696
传真：010-65016411
网址：www.jowto.com