ASC

应用安全联盟

2016 移动物联网安全高峰论坛

新形势下如何做好网际安全防范

孙政豪

安全现状

- 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
- 研发商在安全领域投入少

安全事件概览

2014年全球十大安全事件四起在中国 网站安全漏洞堪忧

《报告》披露,2014年,各类网站存在后门的比例和绝对数量大幅攀升。统计发现,截至2014年11月30日,在164.2万个各类网站中,存在安全漏洞的网站为61.7万个,占被扫描网站总数的37.6%;存在高危安全漏洞的网站共有27.9万个,占扫描网站总数的17.0%;在后门检测中,约3465台服务器存在后门,占比41.2%,比2013年增加了7.4个百分点。

《报告》还总结了2014年全球范围内的十起网站安全事件,包括"openssl心脏出血漏洞"、"ebay数据泄露"、"索尼被黑客攻击"等,在去年的网站安全事件中"121中国互联网dns大劫难"、"携程漏洞事件"、"中国快递1400万条信息泄露"、"12306用户数据泄露"四起发生在中国。

常见的网络层DOS攻击方式

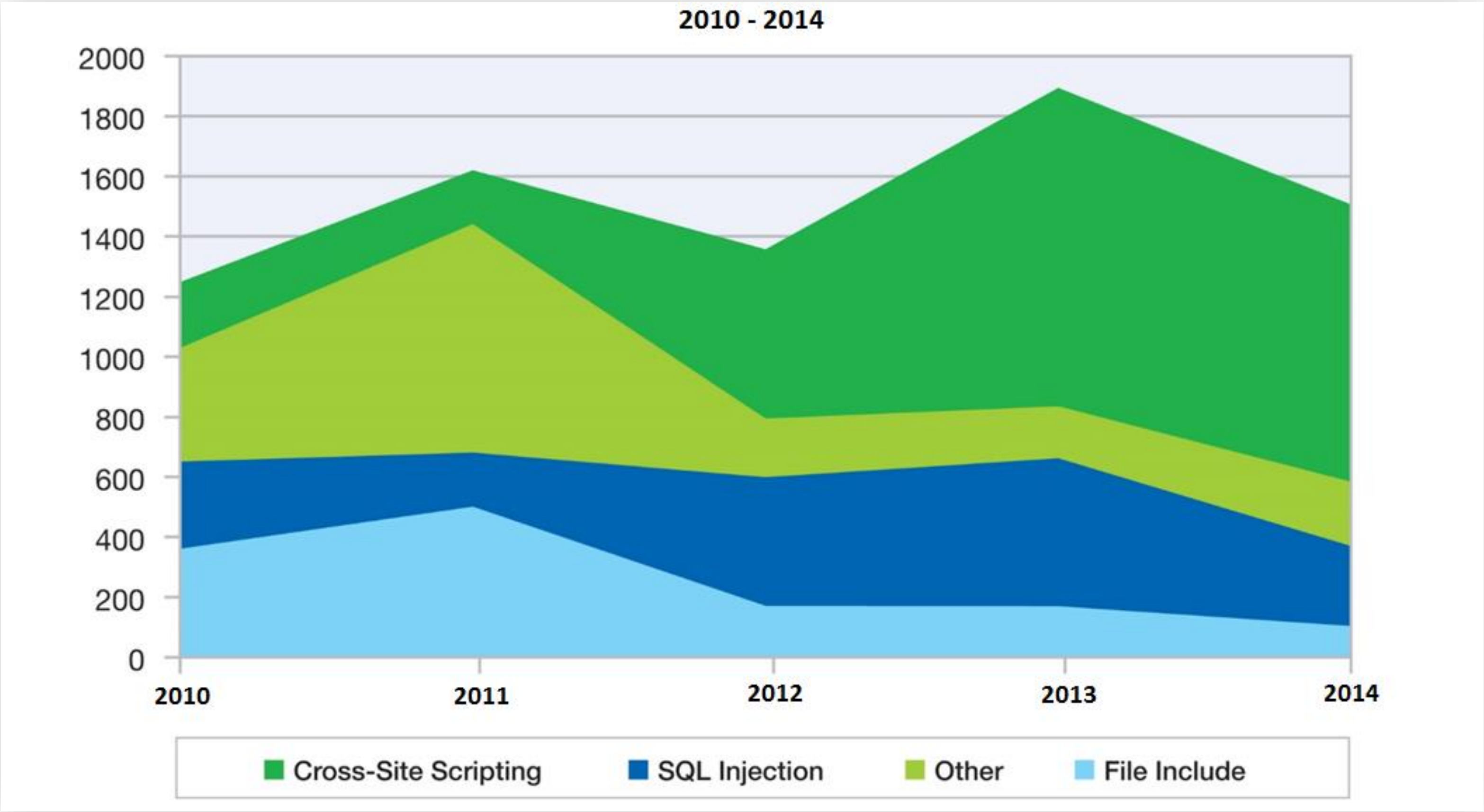
- Ping of Death
- Teardrop
- Flood
- Land
- Smurf
- 分布式拒绝服务攻击

网络空间是一个非常危险的领域 ....

常用的应用层攻击方式

- 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（开发Web应用安全项目）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*

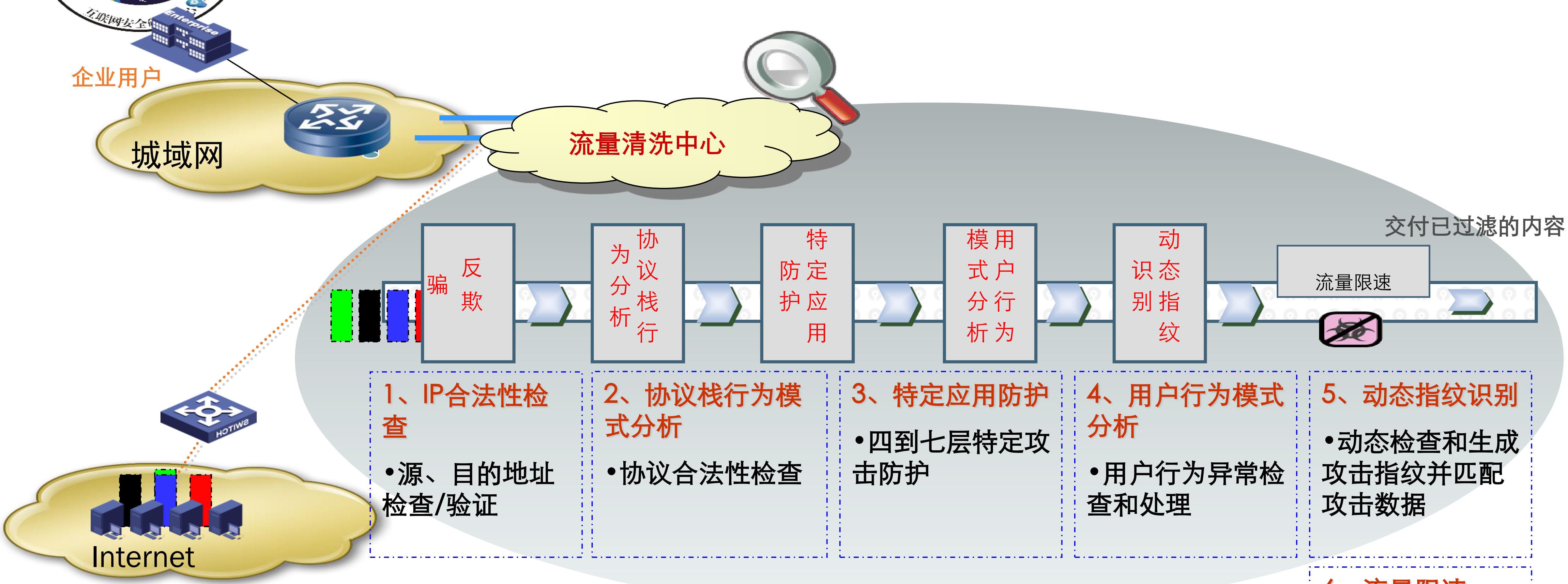
常见的防护方法

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



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

安全软件开发生命周期-SSDLC

需求
- **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**
- 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**

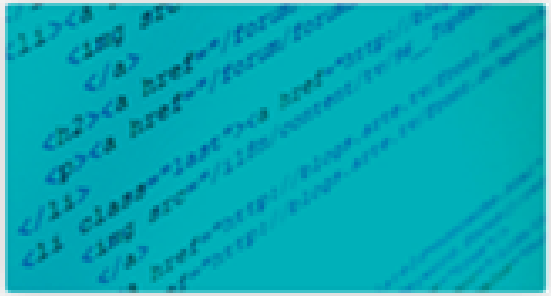
实现
- **标准、检验、工具**
- 遵从安全编码规范
- 使用安全扫描工具 (fuzzing tools, static-analysis tools, etc)

验证
- **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

发布
- **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**

响应
- **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.)

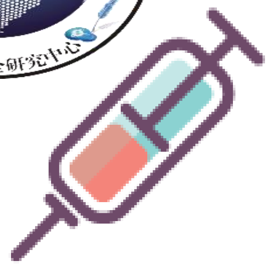
实时应用自我保护技术（Runtime Application Self - Protection）也称RASP技术，是2014年9月Gartner的调研员Feiman提出的一种全新概念。

报告指出，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技术打**虚拟补丁**，来保护你的应用程序



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

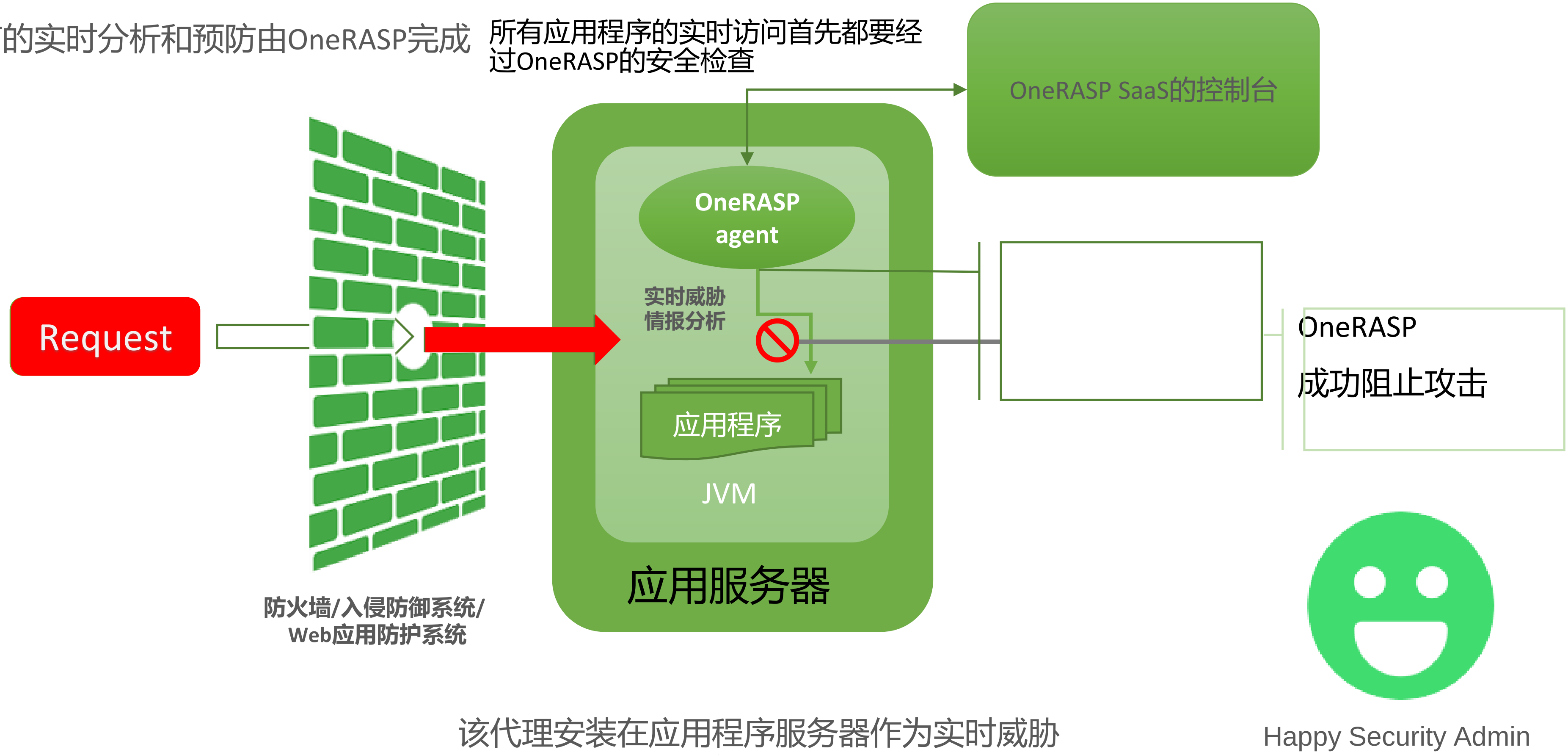
结合应用的逻辑和数据流，在运行时对访问应用的代码进行检测

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

OneRASP请求实例图

所有的实时分析和预防由OneRASP完成

所有应用程序的实时访问首先都要经过OneRASP的安全检查



该代理安装在应用程序服务器作为实时威胁智能筛选器

对企业安全的建议

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。

Q&A

欲了解更多，请访问以下网址

www.oneasp.com

谢 谢！