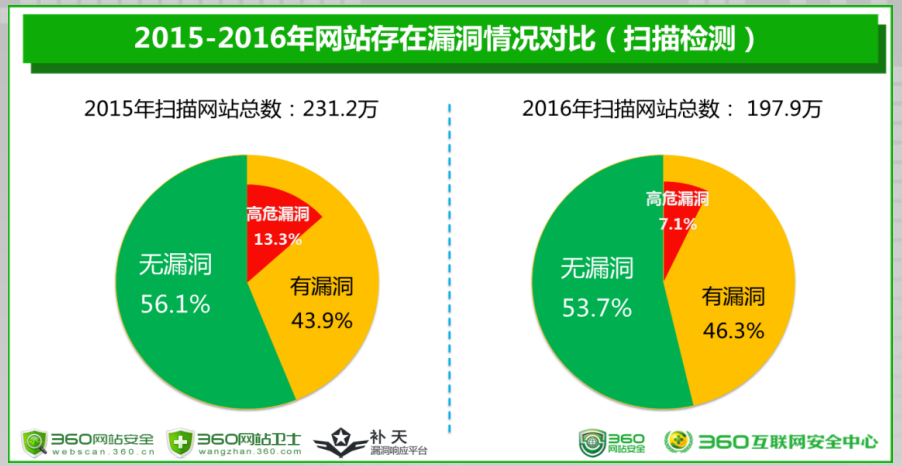
OWASP

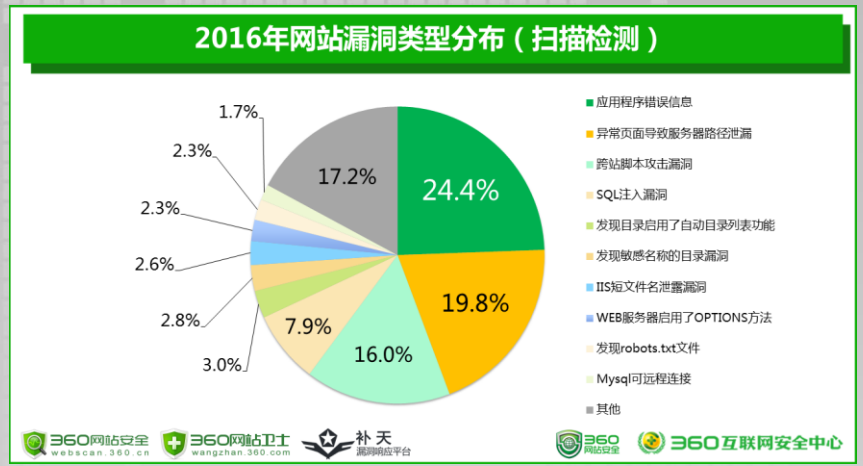
Open Web Application Security Project

云端联动，满足Web安全进阶要求

张盼

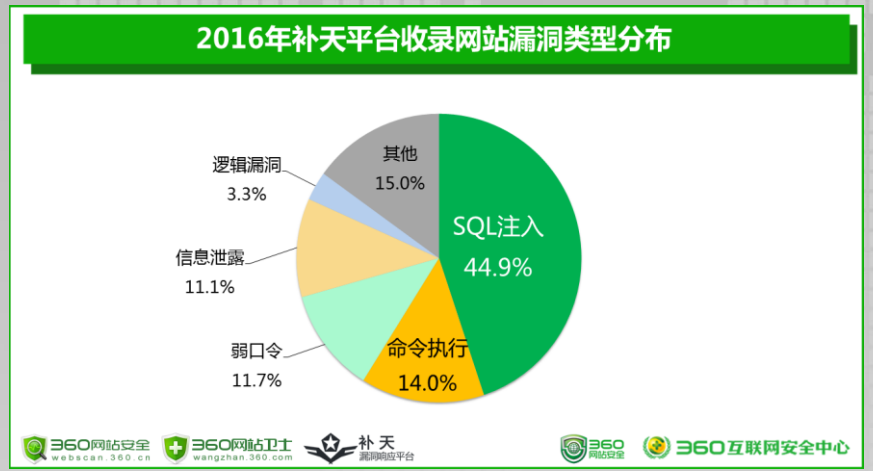
数据分析：2016年网站漏洞数据分析

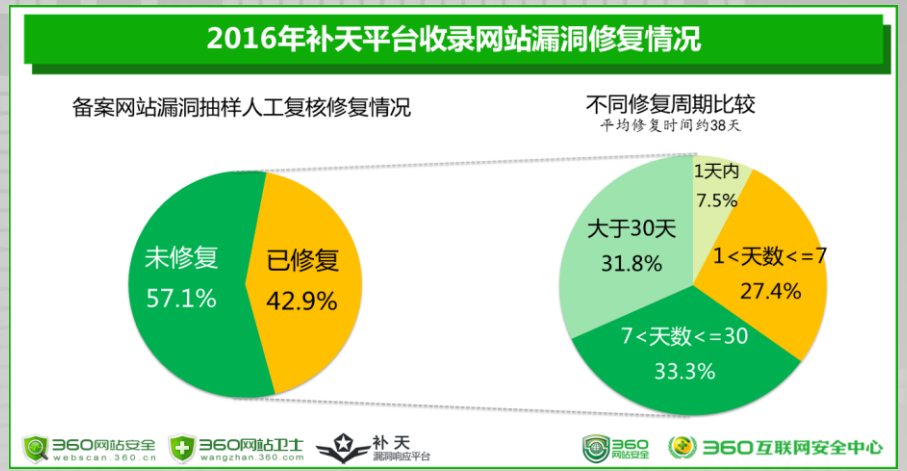




“应用程序错误信息”漏洞是低危漏洞，改变了以前高危漏洞稳居排名第一的局面

数据分析：2016年网站漏洞数据分析





收录漏洞数

2016年：37188个；

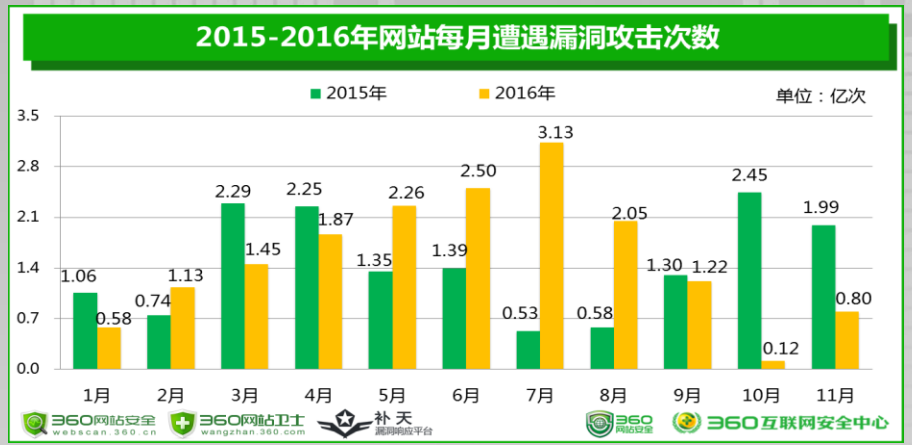
2015年：37943个；

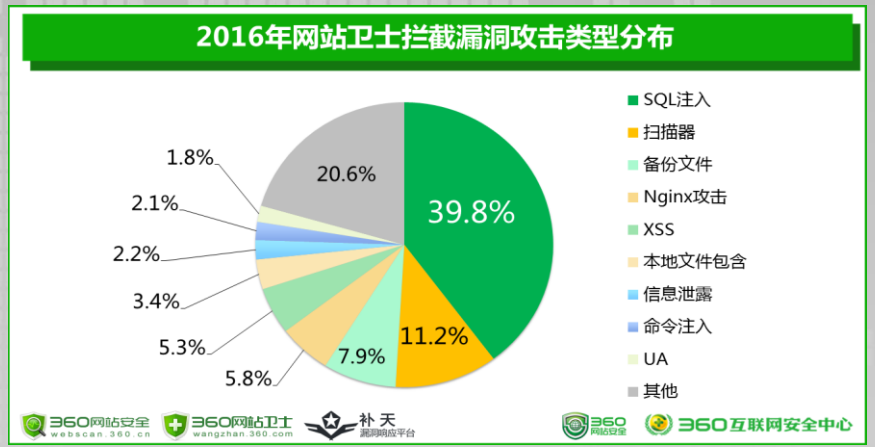
涉及网站数

2016年： 30329个；

2015年： 26370个；

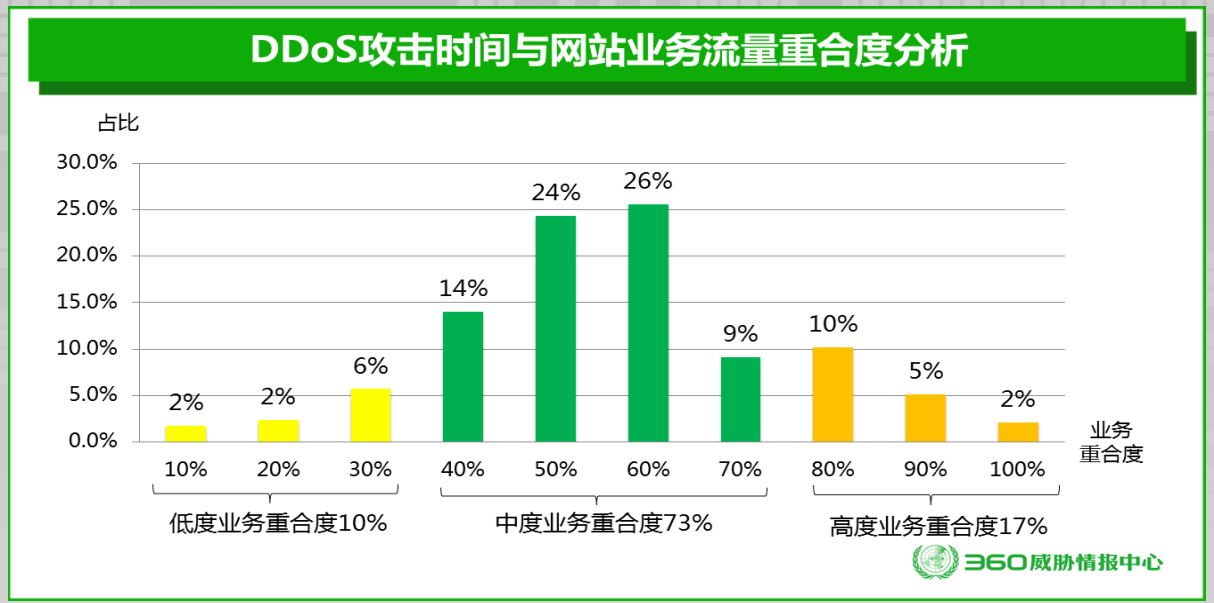
数据分析：2016年网站漏洞攻击数据分析





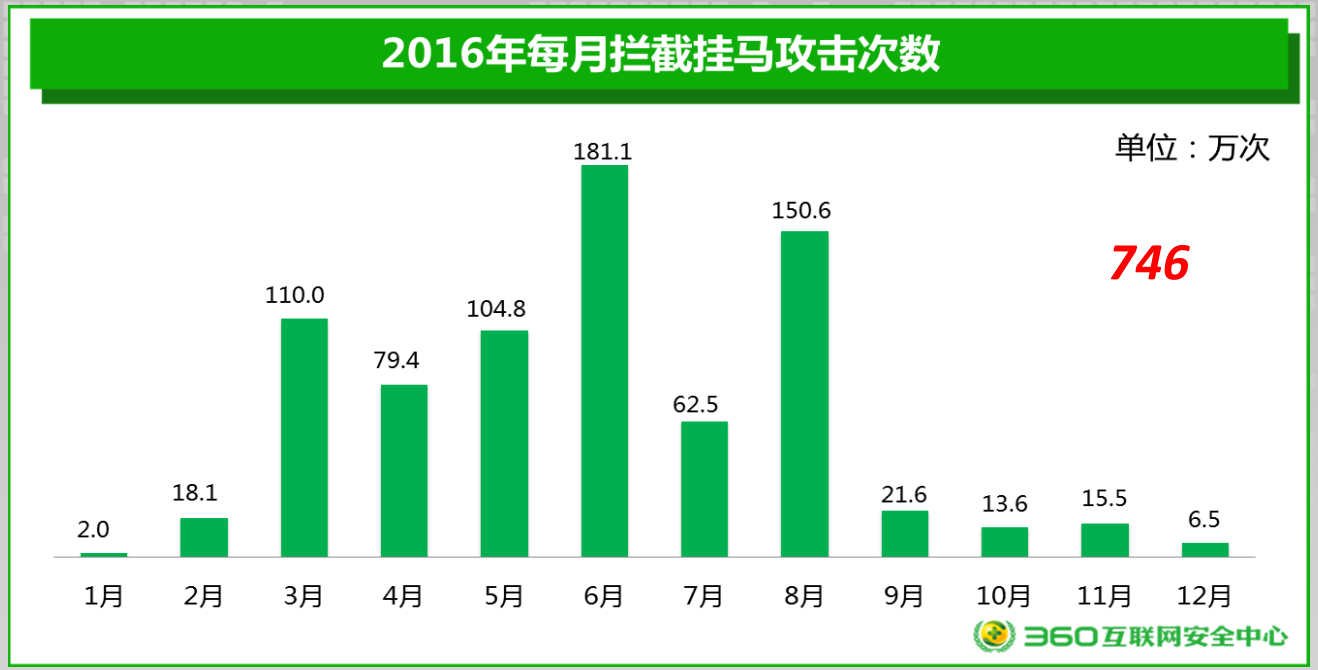
2016年，360网站卫士共拦截各类网站漏洞攻击17.1亿次，较2015年16.5亿次，增长了约3.7%

数据分析：2016年网站DDoS攻击数据分析



攻击时间与被攻击网站的业务流量高峰时段高度重合，重合度在80%以上

数据分析：2016年挂马事件



Web安全——2017

高危漏洞再爆出	• Apache Struts2 再爆出高危漏洞。
勒索成常态	• “无敌舰队”持DDoS攻击勒索多家金融机构； • “永恒之蓝”勒索蠕虫全球泛滥。
法规政策新出台	• 《网络安全法》要求落实等级保护制度； • 国务院《网站发展指引》发文对网站安全建设的细化要求。

360公司的技术实力：漏洞挖掘能力

- 1st 挖掘 VMware VM Escape 漏洞
- 1st 挖掘 Tesla 漏洞
- 1st 挖掘 Google Pixel 漏洞
- 在Pwn2own and PwnFest获得6个冠军

2015 Vulnerability Discovery					
TOP10	Adobe	Apple	Google	Microsoft	Total
Google Project Zero	101	44	2	94	241
ZDI	55	24	0	155	234
360	**55**	**9**	**9**	**26**	**99**
Bilou/Nicolas Joly	42	0	0	0	42
Palo Alto Networks	1	1	0	34	36
Baidu	0				
Trend Micro	5				
Versign iDefense	0				
Keen Team	8				
FireEye	1				

Thanks from Google in 2016			
Team	Android	Chrome	Total
360	**155**	**2**	**157**
Google	74	1	75
Trend Micro	41	5	46
Tencent	21	11	32
Alibaba	28	0	28
Scott Bauer	20	0	20
Rob Wu	0	17	17
Mariusz Mlynski	0	15	15
Michal Bednarski	9	0	9
OUSPG	0	9	9

360公司的技术实力：大数据应用能力

全球文件样本库
- -每天新增900万样本
- -总样本数100亿+
- -20亿+黑名单
- -1亿+白名单

文件行为库（主防）
- -总日志数18.9万亿条
- -每天新增380亿条

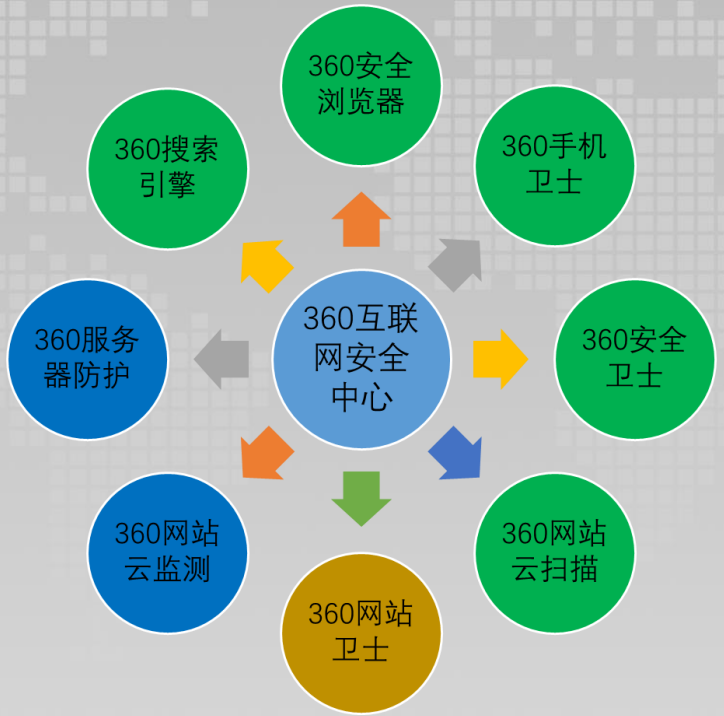
最大中文漏洞库（众测模式）

最大的存活网址库
- •每天查询300亿条
- •每天处理100亿条
- •每天拦截用户访问钓鱼数超过1.4亿URL

互联网域名信息库
- -90亿DNS解析记录
- -每天约新增100万条
- -13年+Whois信息存储
- -约占中国25%DNS解析与查询记录

- 数据来源：全球6亿PC安全客户端，8亿移动端安全客户端；360浏览器、搜索终端应等
- 数据来源：互联网基础设施DNS，猎网、补天等各类举报与响应平台，以及 100+第三方数据源
- 大数据服务器规模超过60000台，总存储数据量接近1.3EB，每天新增超过1.5PB
- 每天各种数据计算任务10万个，每天处理数据量10PB

360公司的社会责任：同时提供面向个人和企业的安全产品



免费

云+端

T10 OWASP Top 10 应用安全风险 – 2017

A1 – 注入	注入攻击漏洞，例如SQL，OS以及LDAP注入。这些攻击发生在当令或者查询语句的一部分，被发送给解释器的时候。攻击者发送的恶器，以执行计划外的命令或者在未被恰当授权时访问数据。
A2 – 失效的身份认证和会话管理	与身份认证和回话管理相关的应用程序功能往往得不到正确的实者攻击者破坏密码、密钥、会话令牌或攻击其他的漏洞去冒充其他用久的）。
A3 – 跨站脚本（XSS）	当应用程序收到含有不可信的数据，在没有进行适当的验证和转发送给一个网页浏览器，或者使用可以创建javaScript脚本的浏览器AP更新现有网页，这就会产生跨站脚本攻击。XSS允许攻击者在受害者从而劫持用户会话、危害网站或者将用户重定向到恶意网站。
A4 – 失效的访问控制	对于通过认证的用户所能够执行的操作，缺乏有效的限制。攻陷来访问未经授权的功能和/或数据，例如访问其他用户的账户，查用户的数据，更改访问权限等。
A5 – 安全配置错误	好的安全需要对应用程序、框架、应用程序服务器、web服务器台定义和执行安全配置。由于许多设置的默认值并不是安全的，因此，必须定义、实施和维护这些设置。此外，所有的软件应该保持及时更新。
A6 – 敏感信息泄露	许多web应用程序和API没有正确保护敏感数据，如财务、医疗保健和PII。攻击者可能会窃取或篡改此类弱保护的数据，进行信用卡欺骗、身份窃取或其他犯罪行为。敏感数据应该具有额外的保护，例如在存放或在传输过程中的加密，以及与浏览器交换时进行特殊的预防措施。
A7 – 攻击检测与防护不足	大多数应用和API缺乏检测、预防和响应手动或自动化攻击的能力。攻击保护措施不限于基本输入验证，还应具备自动检测、记录和响应，甚至阻止攻击的能力。应用所有者还应能够快速部署安全补丁以防御攻击。
A8 – 跨站请求伪造（CSRF）	一个跨站请求伪造攻击迫使登录用户的浏览器将伪造的HTTP请求，包括受害者的会话cookie和所有其他自动填充的身份认证信息，发送到一个存在漏洞的web应用程序。这种攻击允许攻击迫使受害者的浏览器生成让存在漏洞的应用程序认为是受害者的合法请求的请求。
A9 – 使用含有已知漏洞的组件	组件，比如：库文件、框架和其他软件模块，具有与应用程序相同的权限。如果一个带有漏洞的组件被利用，这种攻击可以促成严重的数据丢失或服务器接管。应用程序和API使用带有已知漏洞的组件可能会破坏应用程序的防御系统，并使一系列可能的攻击和影响成为可能。
A10 –未受有效保护的API	现代应用程序通常涉及丰富的客户端应用程序和API，如：浏览器和移动APP中的JavaScript，其与某类API（SOAP/XML、REST/JSON、RPC、GWT等）连接。这些API通常是不受保护的，并且包含许多漏洞。

威胁代理	攻击向量	安全弱点		技术影响	业务影响
应用描述	可利用性 易	普遍性 常见	可检测性 平均	影响 中等	应用/业务描述
任何具有网络访问权限的人都可以向你的应用程序发送一个请求。你的应用程序能检测到手动攻击和自动化攻击并做出响应吗？	已知用户或匿名用户发动攻击。应用程	应用程序和API无时无刻都在遭受着攻击。它们检测到非法输入后，只是丢弃		许多成功的攻击都起始于探测漏洞。	对于业务应该考虑到应对攻击防护不的影响。成功的可能不会被阻很长时间未被并远远超出预

我如何防止？

充分的攻击防护应该包括以下三点内容：

1. **检测攻击**。合法用户不可能做的事情发生了吗（如合法用户不可能创造出的输入）？正常用户是否用永远不会这样使用应用系统（如输入速度过快，不合规则的输入，非正常的使用模式，重复的请求）？
2. **响应攻击**。日志和通知对于及时的响应异常重要。考虑对于某个IP或者一个IP网段是否实施自动阻止。考虑对哪些异常的用户账号进行禁用或者监控。
3. **快速打补丁**。如果你的开发团队不能在一天内对高危漏洞发布补丁，可以尝试部署一个虚拟补丁来分析HTTP流量，数据流，代码执行并且防止漏洞被利用。

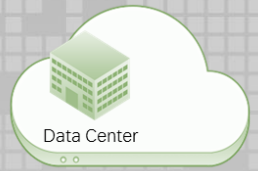
网站安全解决方案：了解现状，监测风险

在第一时间发现网站安全问题

网站安全解决方案：云 + 端纵深防御体系

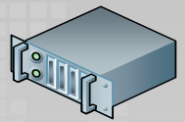
威胁情报中心
- IP信誉
- 0day漏洞信息 / 规则
- ……

SaaS云防护
- DDoS 防护(L3~L7)
- WAF (OWASP TOP10)
- Cache
- DNS防护
- 弹性防护
- 支持多租户管理



本地防护节点
10G ~ 600G

本地防护节点
- DDoS 防护(L3~L7)
- WAF (OWASP TOP10)
- Cache
- 与云端联动，构成混合云
- 支持多租户管理



硬件/ VM image
100M ~ 10G

WAF - Appliance / VM image
- 与云端联动，构成混合云

服务器端软件

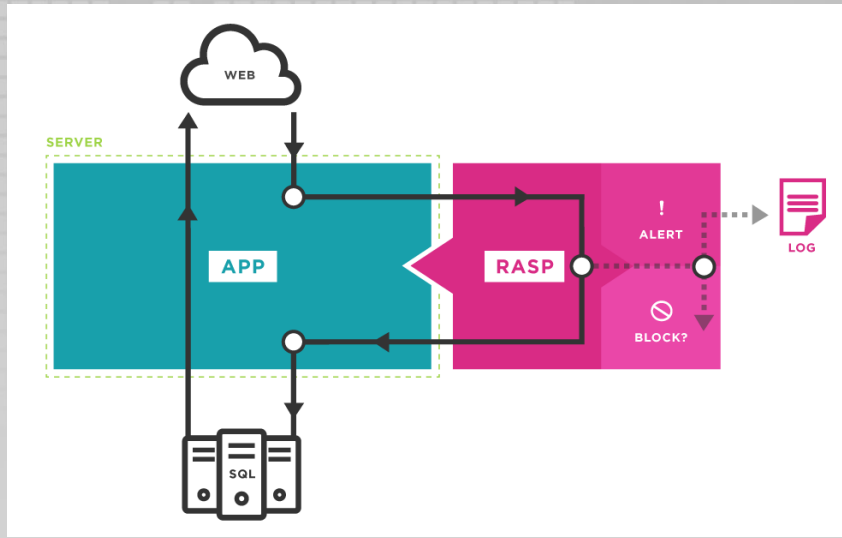
服务端软件
- RASP
- 文件防篡改
- Webshell防护

尝试应用防御新手段：RASP

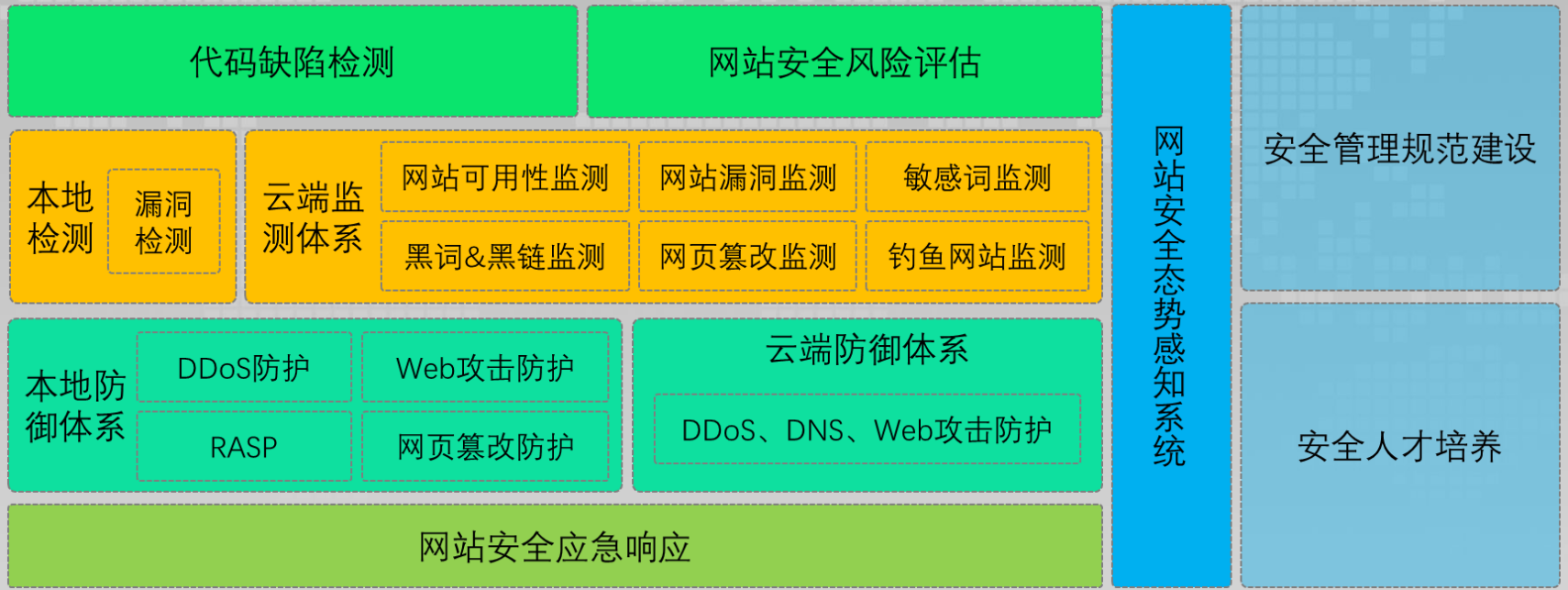
Runtime Application Self-Protection，中文叫做实时应用系统自我保护技术。

RASP是一种新型应用安全保护技术，将保护程序像疫苗一样注入到应用程序，和应用程序融为一体，能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进行自动重新配置应对新的攻击。

综上，RASP 将安全保护逻辑嵌入到运行中的服务器应用程序，它会实时截获所有的系统调用并确保调用安全，最终实现应用程序自我保护。



面向企业的Web安全整体框架



Web安全进阶

国家	• 对网络安全重视程度增加了、要求也更严格更细化了
用户	• 安全意识提升了、对安全的要求提高了
“敌人”	• 能力提高了、目标更统一明确了
人才	• Web安全越来越需要人的参与，人才需求量大增是大趋势
安全行业	• 能力提高了、望多交流、多分享、共同提高
360公司	• 在此抛砖引玉，恳请批评指正