

安世加

AFSS-亚太金融安全峰会

护驾金融，安定民生

上海站 | 2021年7月23日





刘沛旻，Imperva资深技术专家，具有十多年安全行业的工作经验，参与过多个重大信息安全项目的规划、建设和实施，行业涉及金融、电信、制造、能源等多个行业。对于企业的关键信息和应用保护有着丰富的经验和独到的见解。

imperva

Web应用安全的发展和未来

刘沛旻
中国区技术经理

讲起Web应用安全

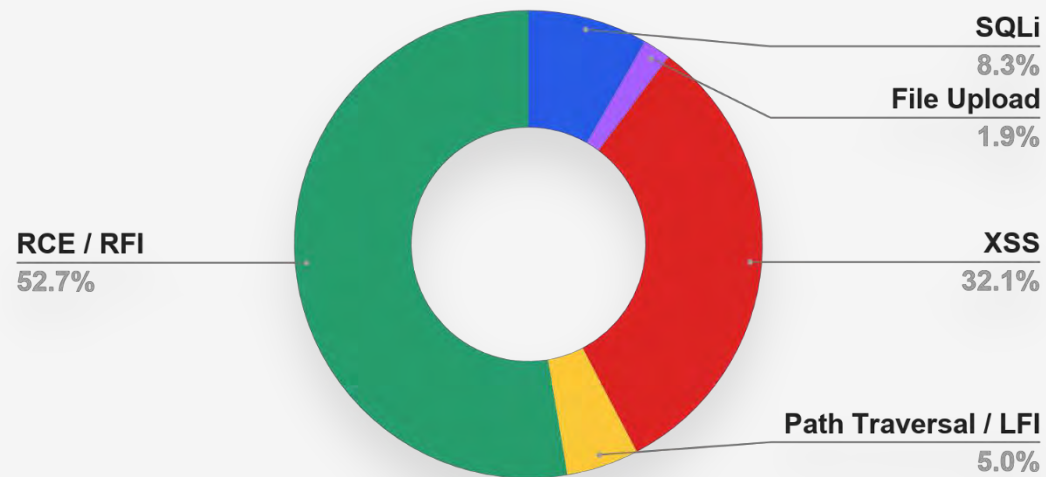
你想到的第一个关键字是什么？

从2003版到2017版

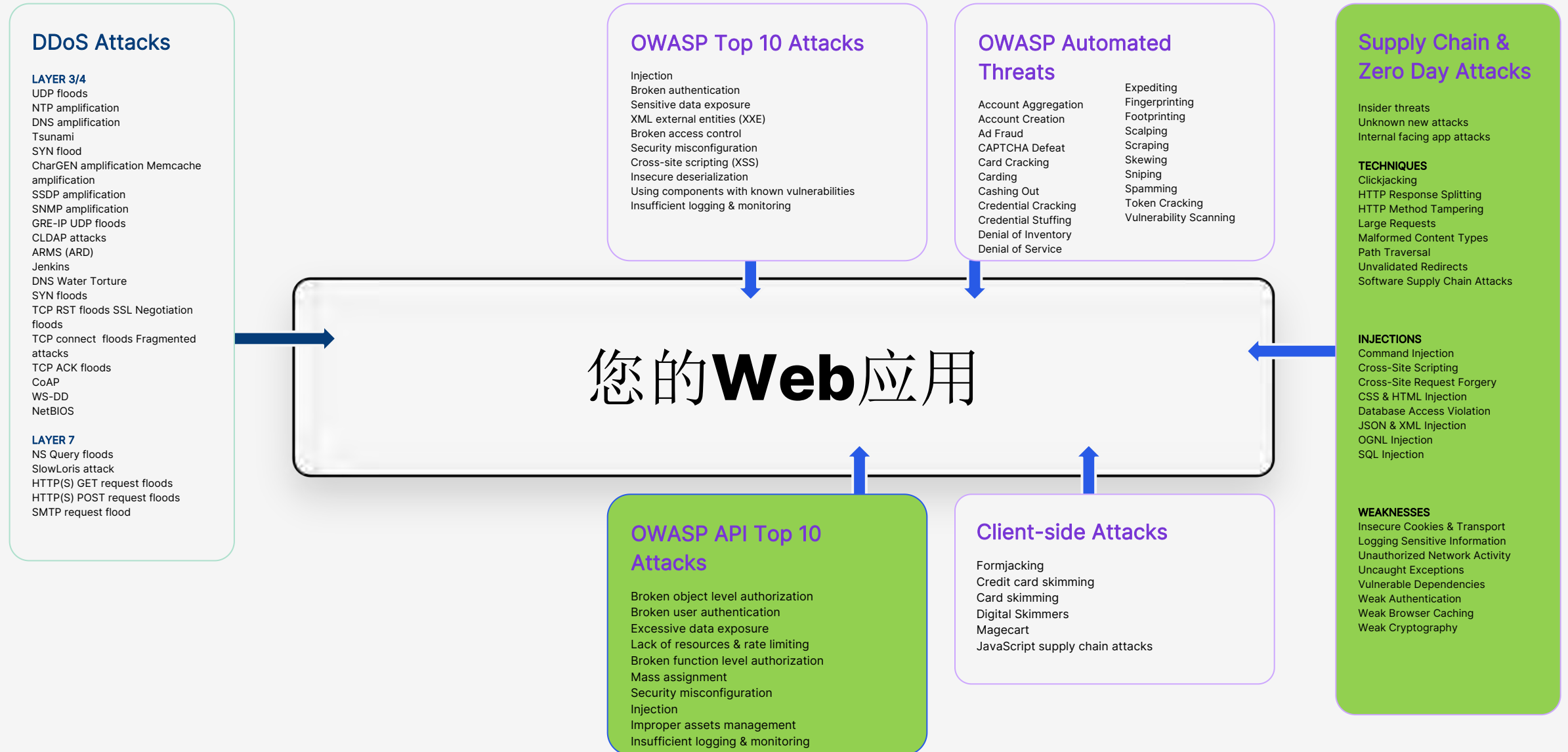


Top 5 的Web应用攻击

Imperva 2020年上半年分析了11.4亿客户请求，其中主要攻击类型分布如下



Web应用安全远不止OWASP TOP10



APIs 已成为攻击者的目标

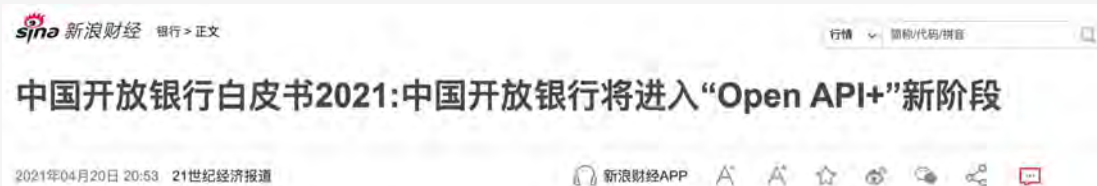
到2022, API 将会成为企业Web应用数据泄露 最常见的攻击向量

Gartner

开放银行：进入**API**新时代

API的安全问题已经成为Web应用安全的重点

- 2018年开始发展
- 开放API与其他银行以及第三方机构共享财务数据
- 安全挑战：
 - API安全
 - 数据隐私



Web应用安全的定义 > WAAP

Web Application and API Protection

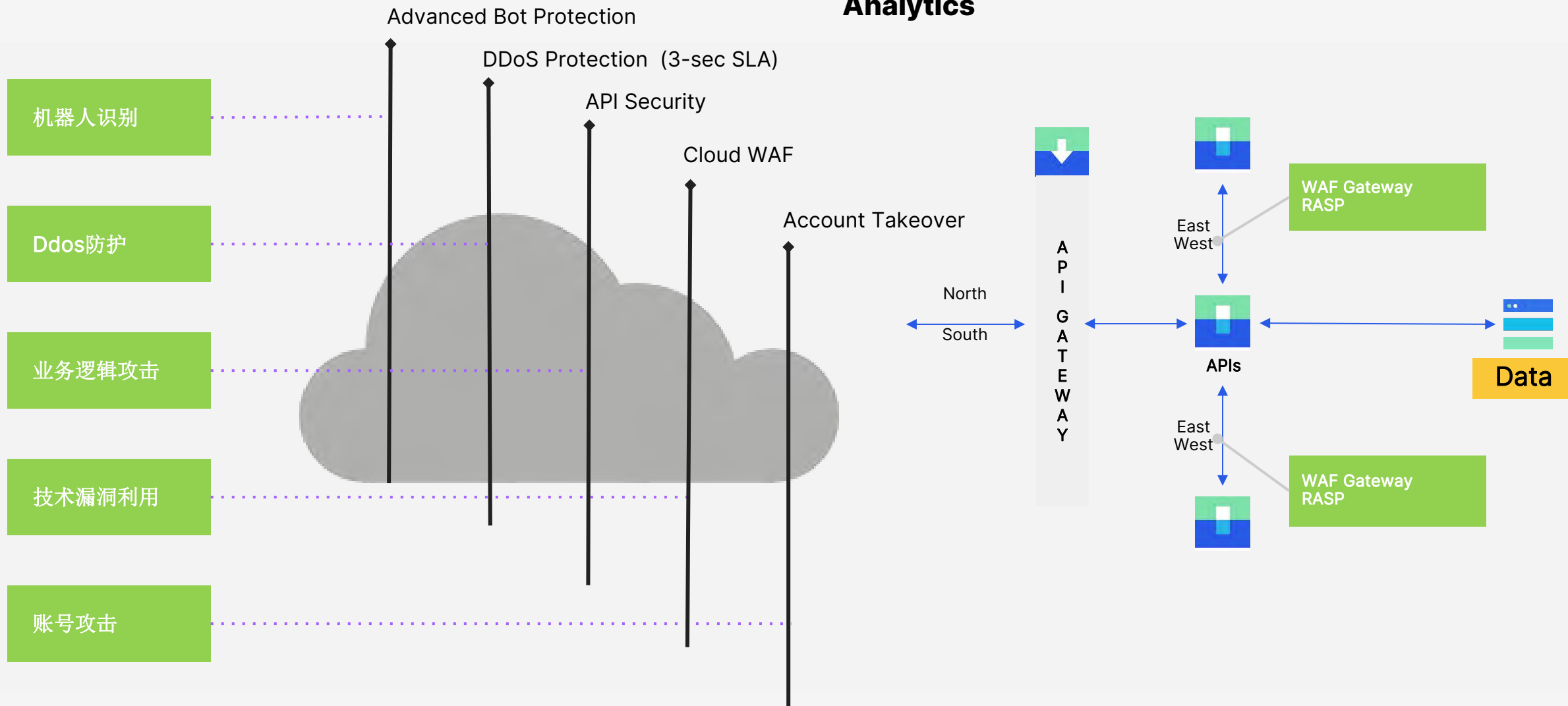
The image is a screenshot of the Gartner Peer Insights website. The page title is 'Web Application and API Protection Reviews and Ratings'. It features a search bar at the top, navigation links, and a section titled 'What is Web Application and API Protection?'. Below this, there is a section for 'Products In Web Application and API Protection Market' with filters for company size, industry, and region. The main content area displays a product listing for 'Imperva Cloud WAF' by Imperva, showing a 4.8 star rating and a brief review snippet.

API 安全最佳实践



**Attack
Analytics**

启发式分析和机器学习



API 安全 vs 传统安全

白名单模型严格控制访问

自动获取 OPENAPI 定义规范 (Swagger)

针对每个API接口进行严格的访问控制

避免API滥用

利用统一的Web应用安全平台进行 APIs 安全管控



软件供应链安全

零日漏洞如何进行防护？

2020年12月，SolarWinds Orion软件系统被俄罗斯黑客利用



这些供应链攻击方法是：

- 攻陷供应商
- 第三方程序利用
- 开源库漏洞利用
- 依赖包混淆
- 恶意的账号接管

永远都可能存在的“后门”

从头开始造轮子 vs 快速开发

第三方组件
漏洞利用

开源库
漏洞利用

Example "Zero-Days" in Common Third Party Software Applications

Microsoft Exchange Server remote code execution	CVE-2021-26412, CVE-2021-26854, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078
SaltStack remote code execution	CVE-2021-3148
Zoho Manage Engine Desktop deserialization / remote code execution	CVE-2020-10189
Microsoft Dynamics 365 cross-site scripting / credential stealing	CVE-2020-0656
Cisco Prime Collaboration Provisioning SQL injection / data access	CVE-2020-3184

Example "Zero-Days" in Common Open Source Components

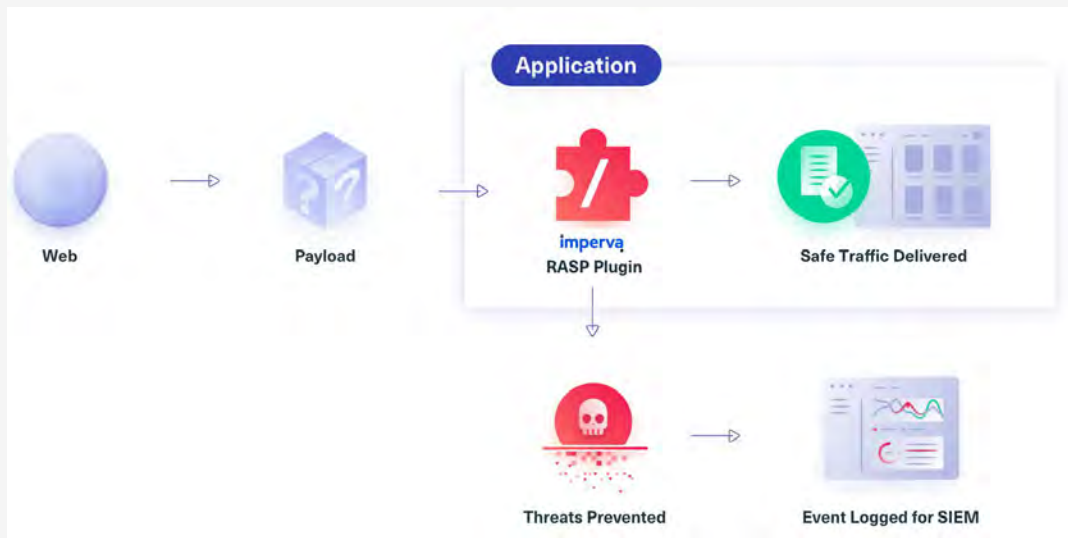
Struts 2 OGNL injection / remote code execution	CVE-2020-17530
FasterXML jackson-databind deserialization / remote code execution	CVE-2020-10968
Apache Camel deserialization/remote code execution	CVE-2020-11972
Microsoft .NET Framework XPS validator / remote code execution	CVE-2020-0605
PostgreSQL jdbc driver XML external entity / remote code execution	CVE-2020-13692

RASP: 给Web应用打上疫苗

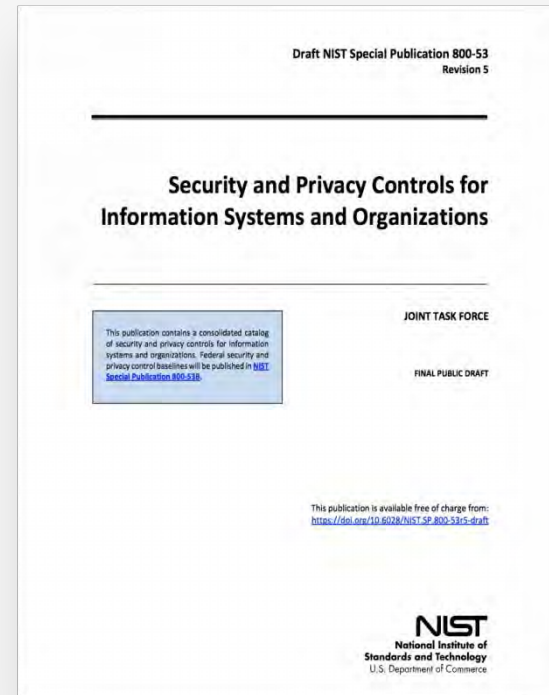
看到程序代码运行的情况

Runtime Application Self-Protection, 实时应用自我保护

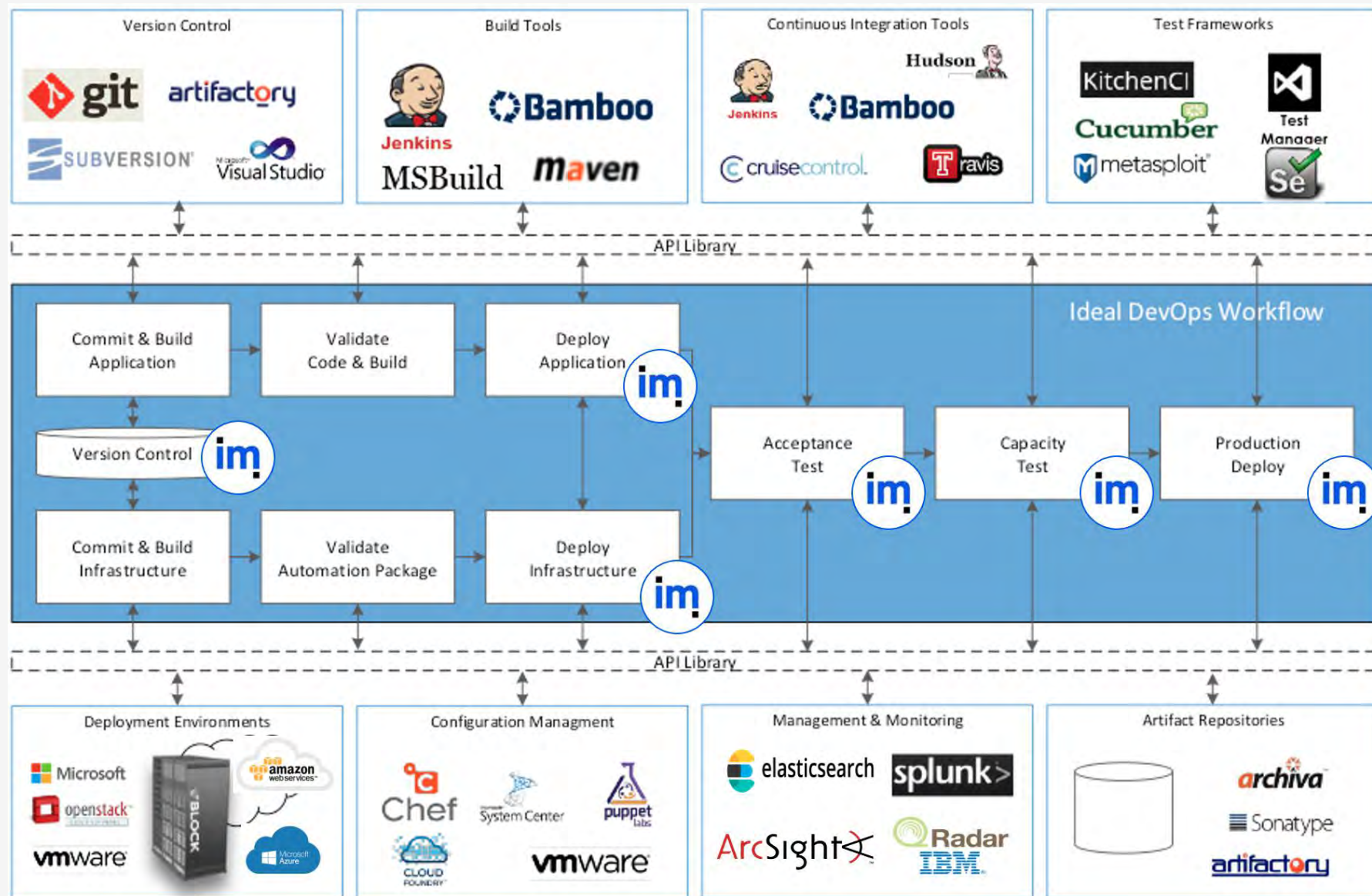
- Secure By Default
- 无需修改代码、程序运行时检测



美国国家标准技术研究院在“信息系统和组织的安全和隐私控制”^{*}中建议使用RASP



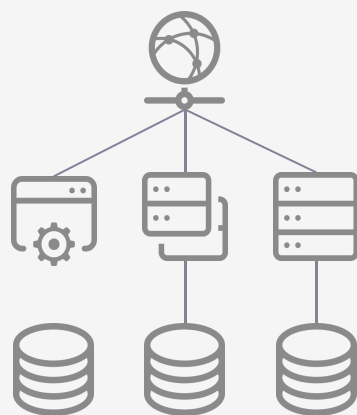
在软件开发的各个阶段开始防护



Web应用安全的未来趋势

更加适应未来Web应用的架构

过去



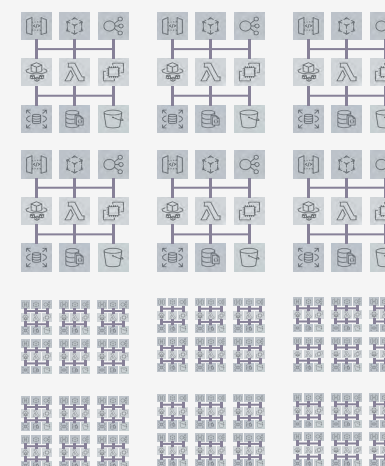
On-Premises

现在



Cloud

未来



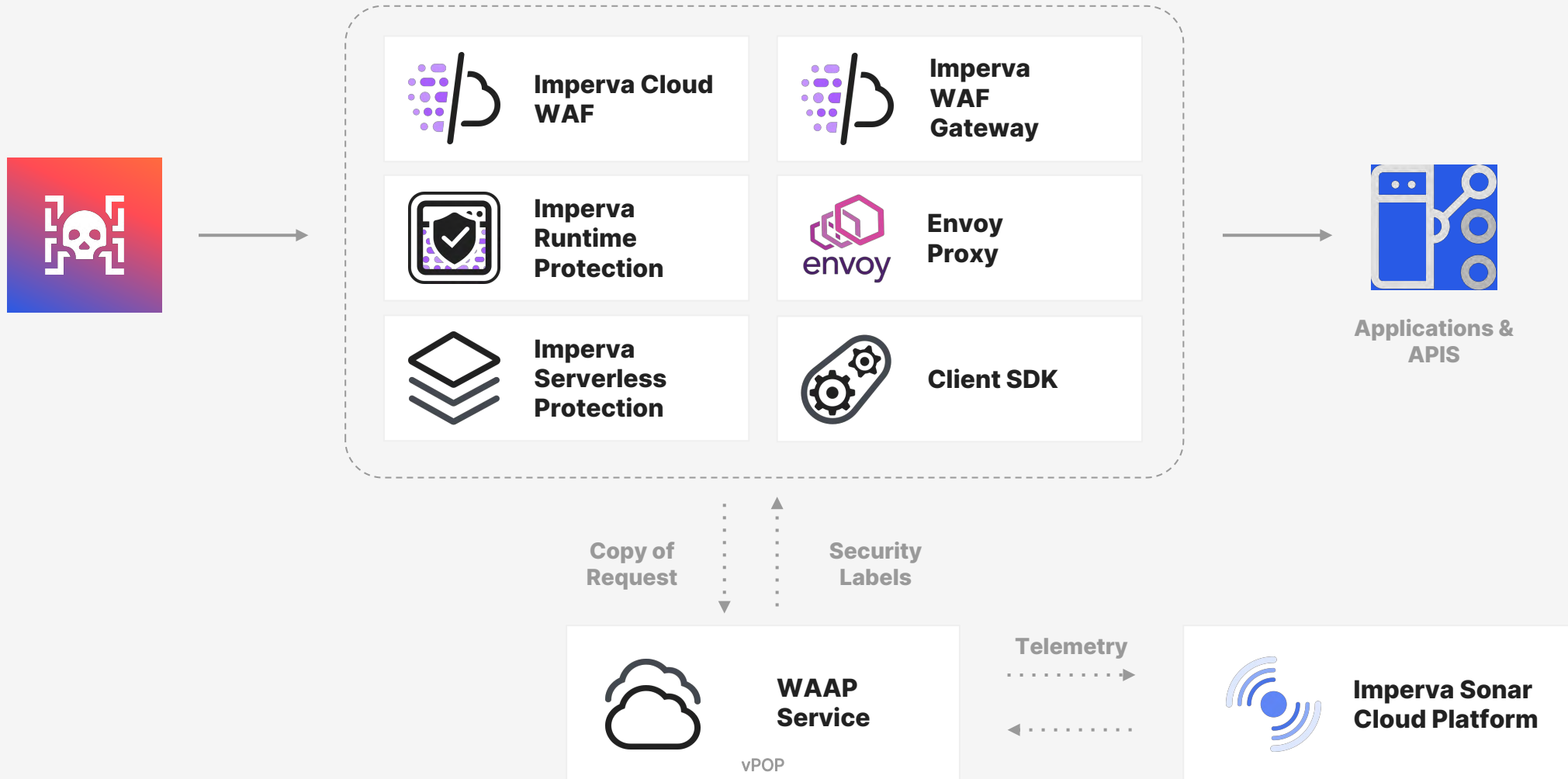
Multi-cloud,
Serverless

WAAP各层次保护手段

	At the Edge	At the Cloud Provider	At the Data Center	At the Service Mesh	At the Workload	At the Function
保护手段	Cloud WAF	集成服务	WAF Gateway	云原生集成	RASP	Serverless保护
安全维度	WAAP 安全服务 API Security, Application Security, Bot, Client-Side Protection, Intelligence & Reputation...					
集成	系统集成 防病毒, API 网关, 云供应商, DevOps 集成, 身份认证供应商, SIEMs...					
管理 & 分析	集中管理和云端分析 统一管理和配置, 机器学习...					

WAAP Anywhere

概念架构



Thank You

安世加专注于安全行业，通过互联网平台、线下沙龙、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：

<https://www.anshijia.net.cn>

微信公众号：asjeiss



安世加