

IMPERVA

云环境下的应用和数据安全实践

Peimin Liu 刘沛旻

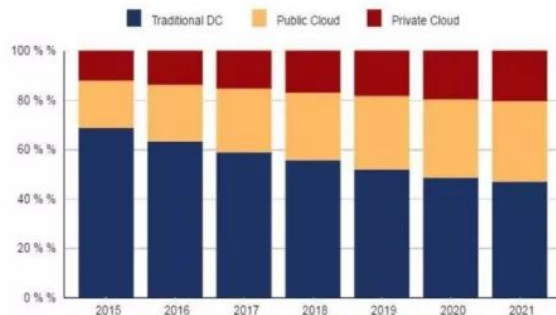
Nov 2018

安全加
IMPERVA

往云端的迁移继续在加速

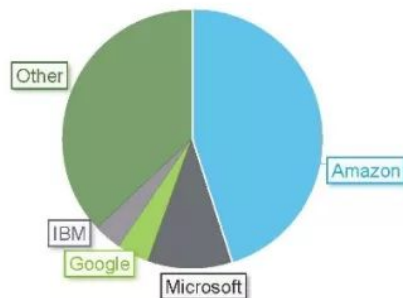


Worldwide Cloud IT Infrastructure Market Forecast
by Deployment Type 2015 - 2021 (shares based on Value)



50% 是云

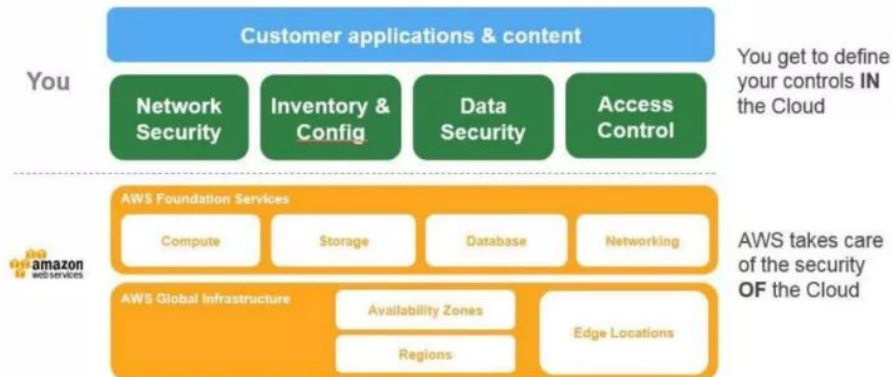
KEY PLAYERS IN CLOUD INFRASTRUCTURE



Synergy Research Group, 2017

在云环境下客户还是需要自己来考虑应用和数据的安全

Customers are responsible for securing the customer applications and content hosted in any cloud infrastructure – AWS, Azure, and others



AWS Article: [Introduction to AWS Security, July 2015](#)

Azure Blog Post: [Cloud Security is a Shared Responsibility, June 2015](#)

云应用上业务的转变

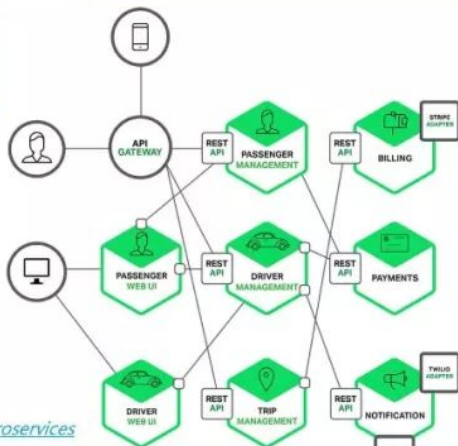
单一化



Source : <https://dzone.com/articles/introduction-microservices>



微服务



云环境下的安全趋势

- 攻击的主要目标是**数据**
- **WEB应用**仍然是安全短板经常被利用，**移动应用安全**问题越来越多
- 攻击变得更**复杂**、更**多样**、更**难检测**
- DDoS攻击的**强度大增**，复杂度大增 – 已经监测到 1Tbps以上 的DDoS攻击
- **API的安全**防护问题
- **DevSecOps**的需求
- 云计算的快速推广给应用及数据带来的新的挑战
 - 部署模式的挑战
 - 自动化、快速部署的挑战
 - 服务化的挑战
 - 缺少匹配的安全运维人员



为企业保护
最关键的应用和业务数据

混合环境下的应用和数据安全架构



Outside the Organization

Good Users

Partners

Customers

Contractors

Bad Users

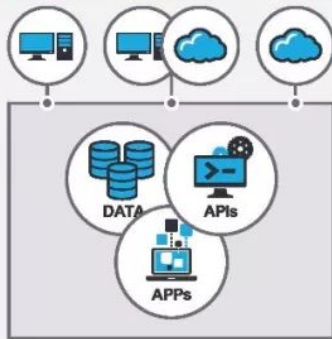
Bad bots

Hackers

SECURE APP DELIVERY

FlexProtect for Applications

ON-PREM HYBRID CLOUD



DATA SECURITY & COMPLIANCE

FlexProtect for Databases



Inside the Organization

Good Users

Trusted

Privileged

Bad Users

Malicious

Careless

Compromised

Analytics & Machine Learning

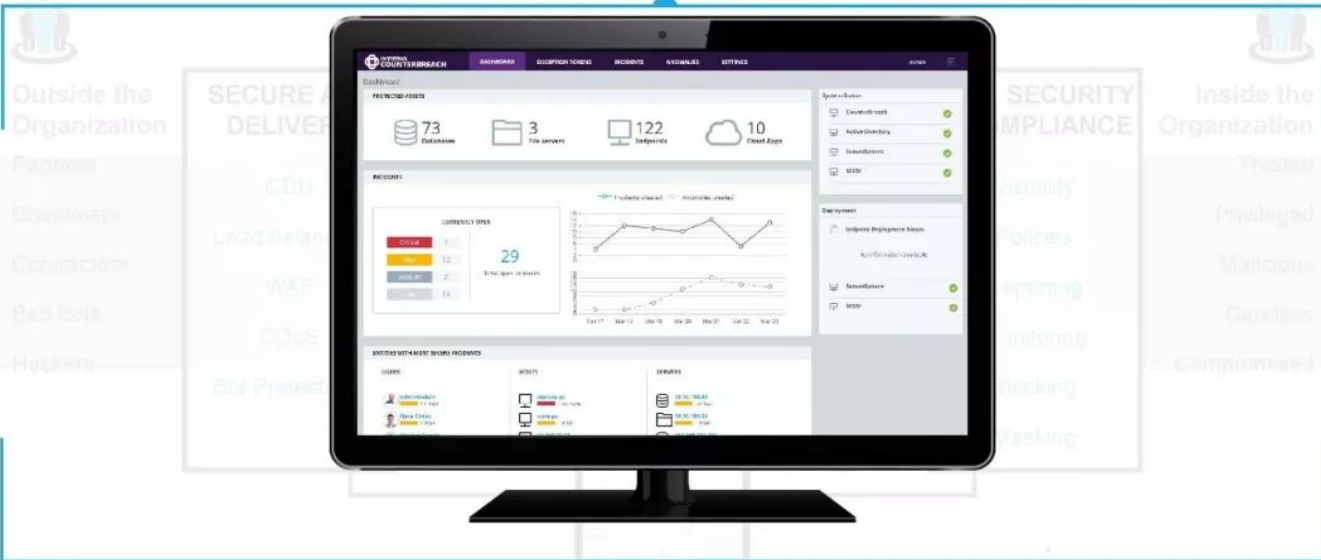


SIEM



Executive Team

BOD, CFO, CIO, Risk Compliance



Execution Team

Manager, IT Director, SOC, SecOps, Network Sec, DBA, Analysts, Network Ops, Architects





Imperva FlexProtect for Applications

- DDoS mitigation
- Threat intelligence
- Anti-automation
- Attack analytics

Imperva FlexProtect for Databases

- Discovery
- Activity monitoring
- Classification
- Insider threat protection

保护云中的应用安全

FlexProtect for Apps

Imperva Application Protection Product Portfolio



Incapsula

- Cloud WAF解决方案
- 提供机器人识别和控制功能
- 提供3-7层Ddos防护能力
- 提供CDN加速服务
- SaaS服务



SecureSphere

- 行业领导者的WAF解决方案
- 提供物理设备、虚拟化、云环境中多种部署模式
- 提供丰富的自定义策略，可根据客户需要定制业务访问控制策略



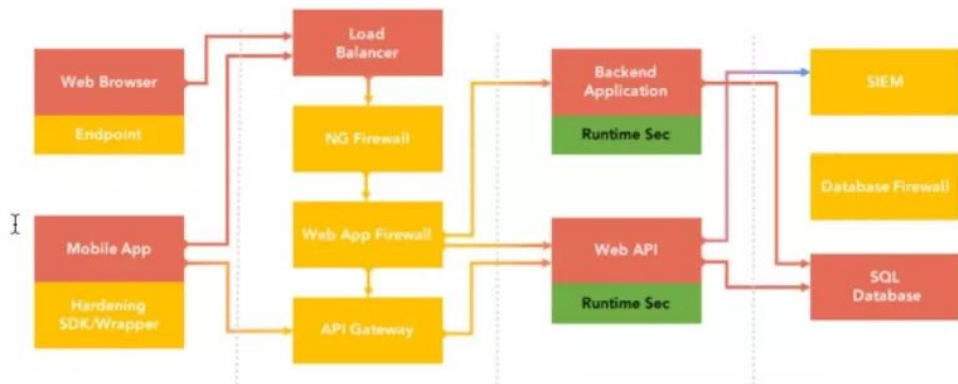
Prevoty

- 行业领导者的RASP解决方案
- 基于专利LANGSEC技术检测运行环境中的攻击行为
- 支持本地插件部署，可支持Java、.NET、Ruby、Node.js等环境

RASP (Runtime Application Self Protection)

The Enterprise Architecture Framework

Figure 1: A typical enterprise using web-based applications as their business



高运维风险
大流量型

高安全风险
技巧攻击型

运行环境风险
东西向攻击



DDoS

信誉和机器人

通用攻击

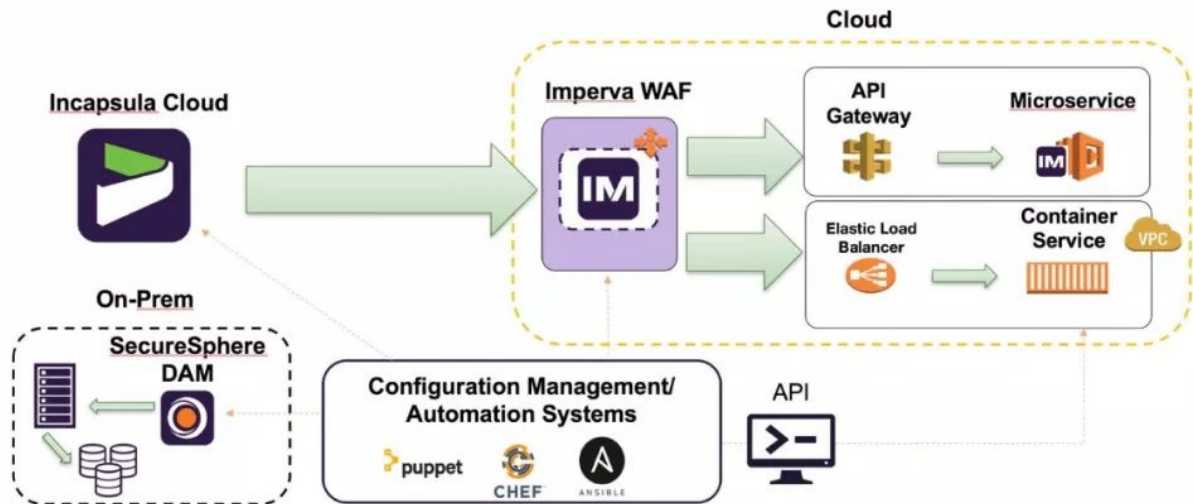
业务层访问控制

逻辑攻击

应用模型

定向攻击

云端Web应用安全防护



利用机器学习解决告警疲劳的问题

- 解决安全告警泛滥的问题
- 解决复杂的告警分析问题
- 解决安全人员紧缺的问题
- 提供聚焦的告警信息和相关的背景信息

Machine Learning



2018 Gartner Magic Quadrant for Web Application Firewalls



2018 Forrester New Wave

Rue time application Self-Protection



保护云中的数据安全

FlexProtect for Data

Imperva Data Protection Product Portfolio



SecureSphere

- 针对数据库、大数据、共享文件的保护解决方案
- 发现数据库漏洞、数据分类
- 监控和审计所有的用户操作行为



CounterBreach

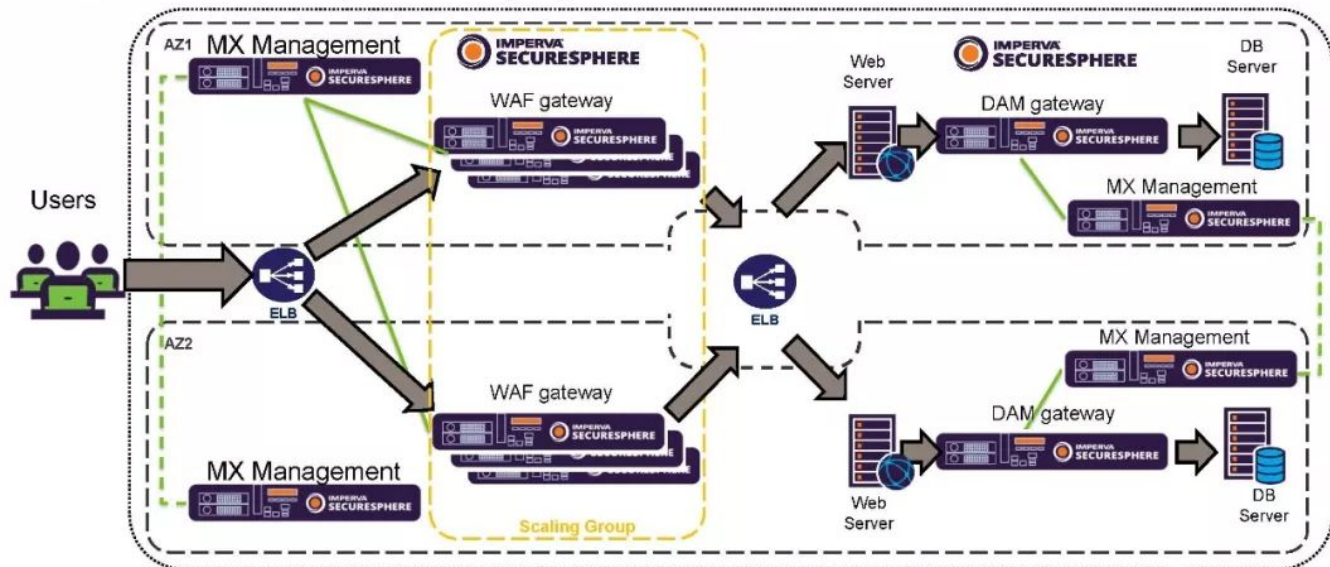
- 基于无监管机器学习的用户行为分析解决方案
- 零安全策略设置
- 自动化侦测各种异常的数据访问行为



Camouflage

- 数据脱敏解决方案
- 使用接近真实的伪造数据替代敏感数据
- 避免敏感数据被非生产系统使用

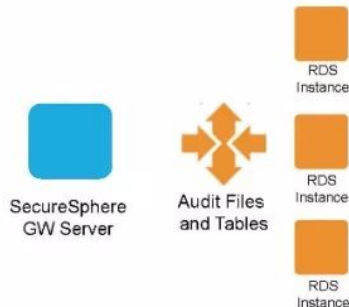
AWS: SecureSphere Deployment Architecture - WAF + DAM



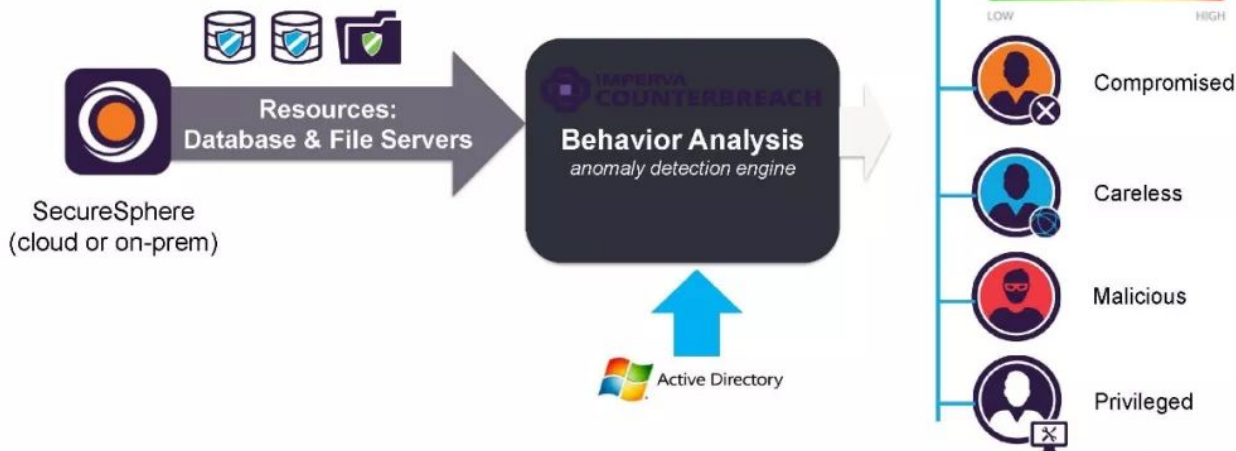
SecureSphere for RDS

- RDS支持

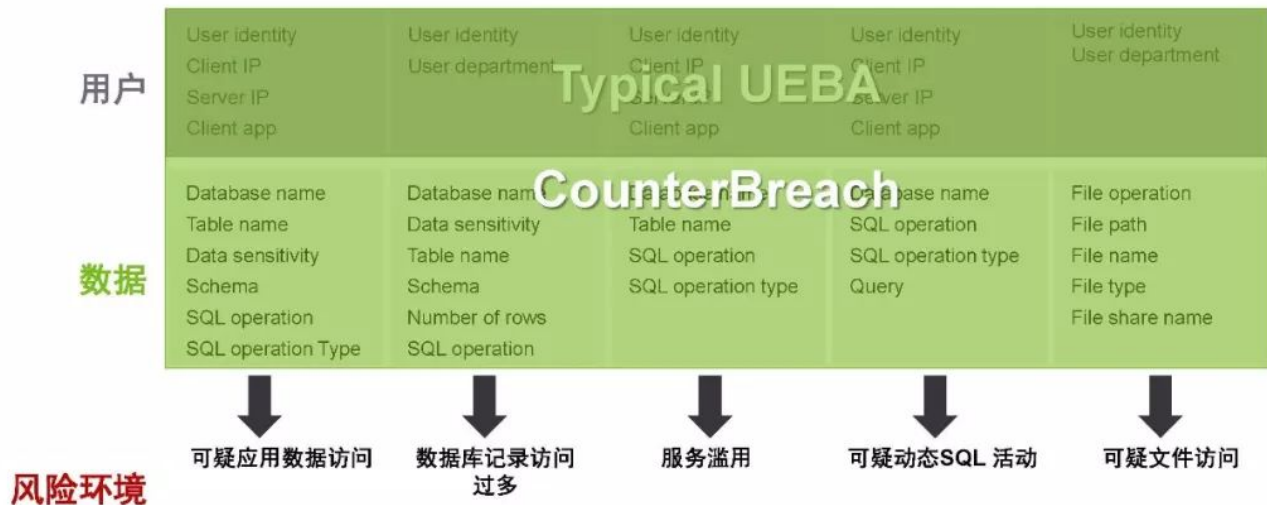
- 采用非Agent模式，采集RDS自身Log日志
- 目前提供Oracle、PostgreSQL引擎
- 统一的日志格式和管理界面



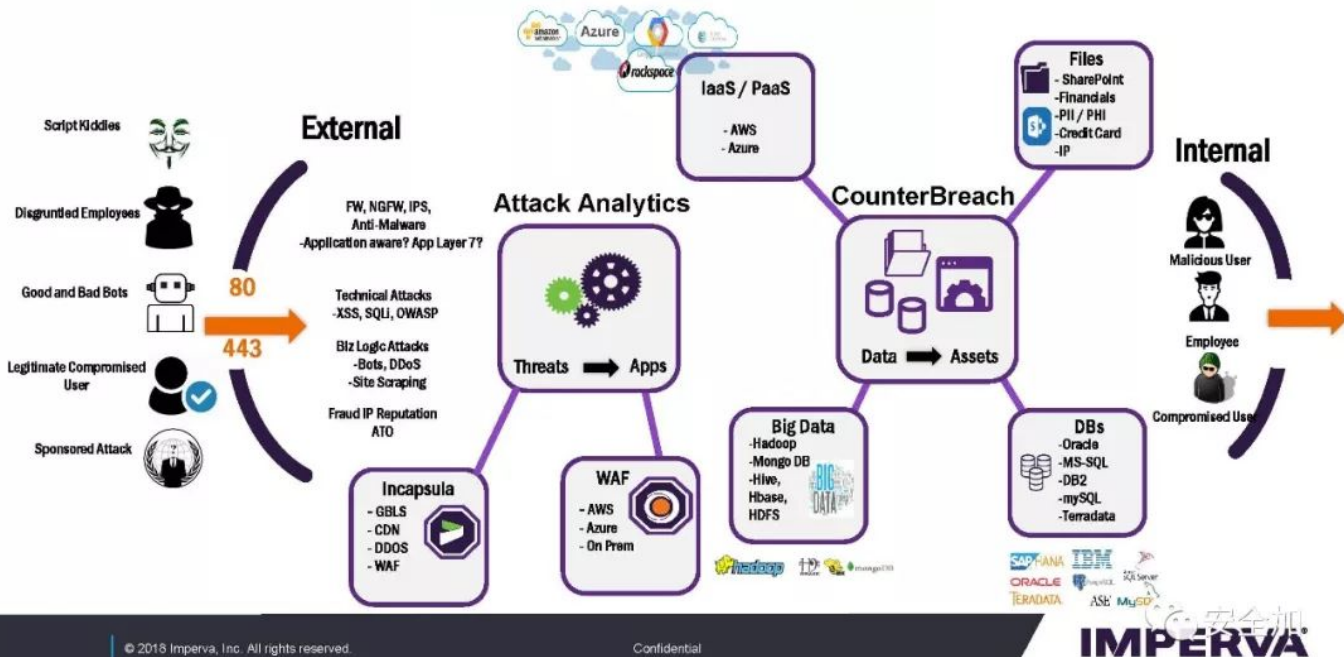
利用CounterBreach统一监控数据违规



根据用户与数据情况识别数据违规



Imperva Reference Architecture



IMPERVA

Thanks