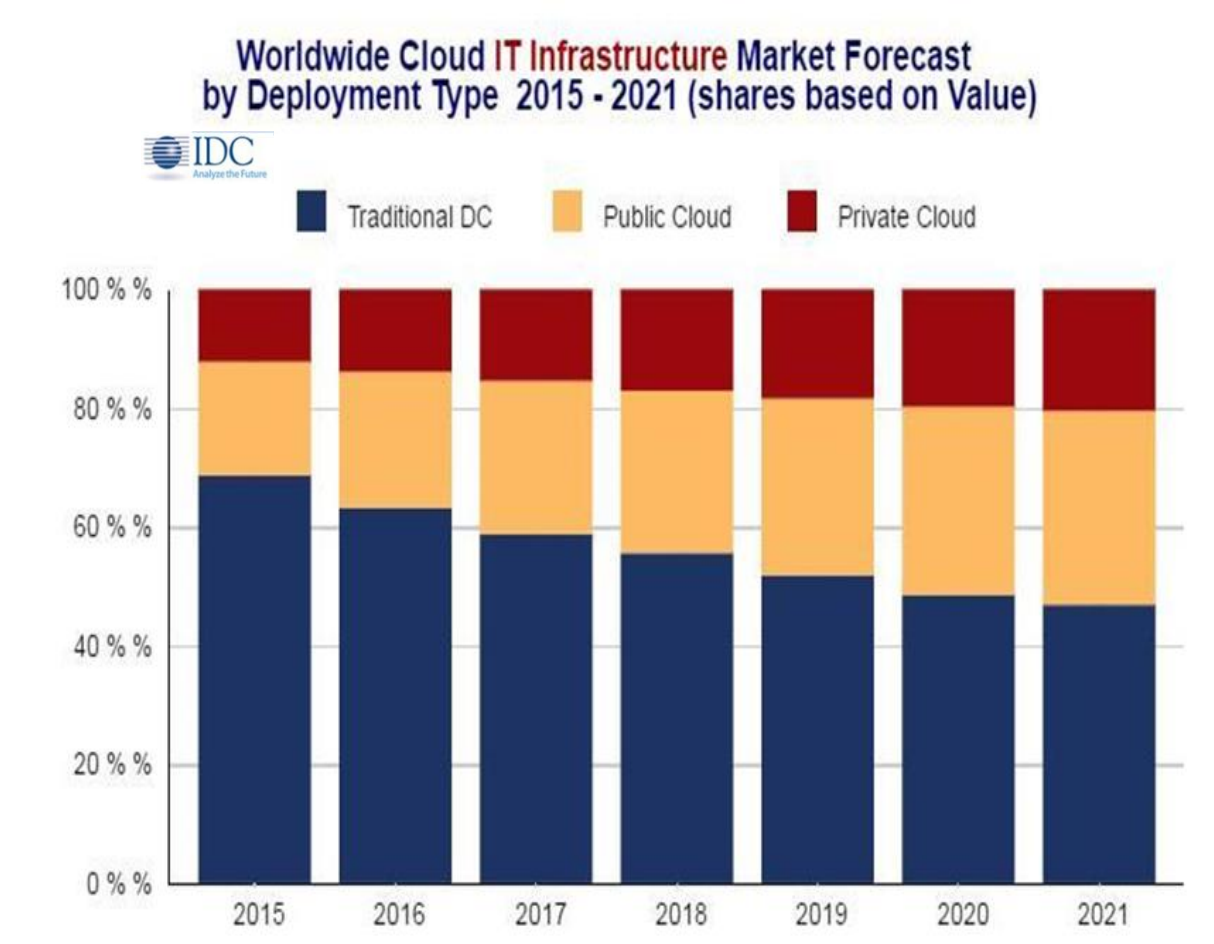
云环境下的应用和数据安全实践

路笑凡

中国区资深技术顾问

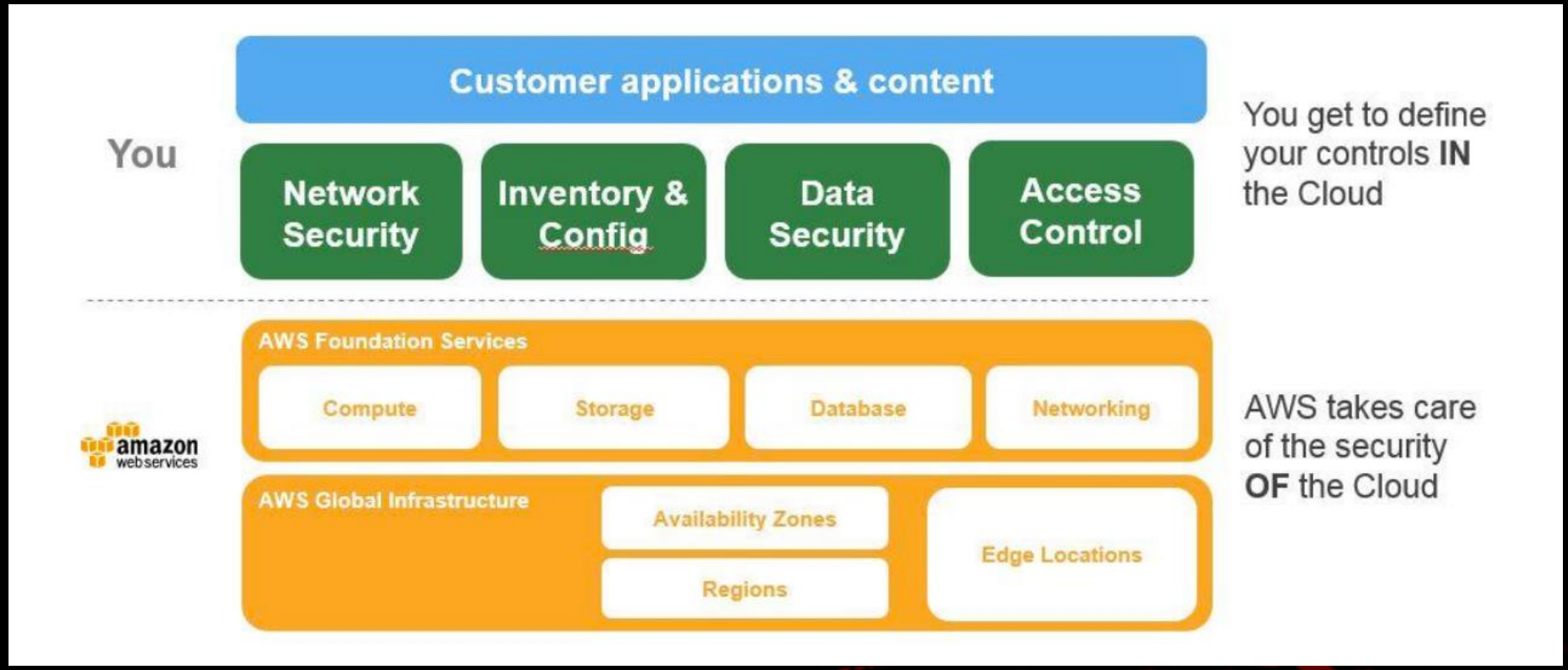
往云端的迁移继续在加速



50% 是云

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



Confidential

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
- DevOps的安全防护问题
- 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
- AI大数据平台联动分析和响应

为企业保护

最关键的应用和业务数据

IMPERVA

保护云中的应用安全

Confidential

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

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

云应用安全模型

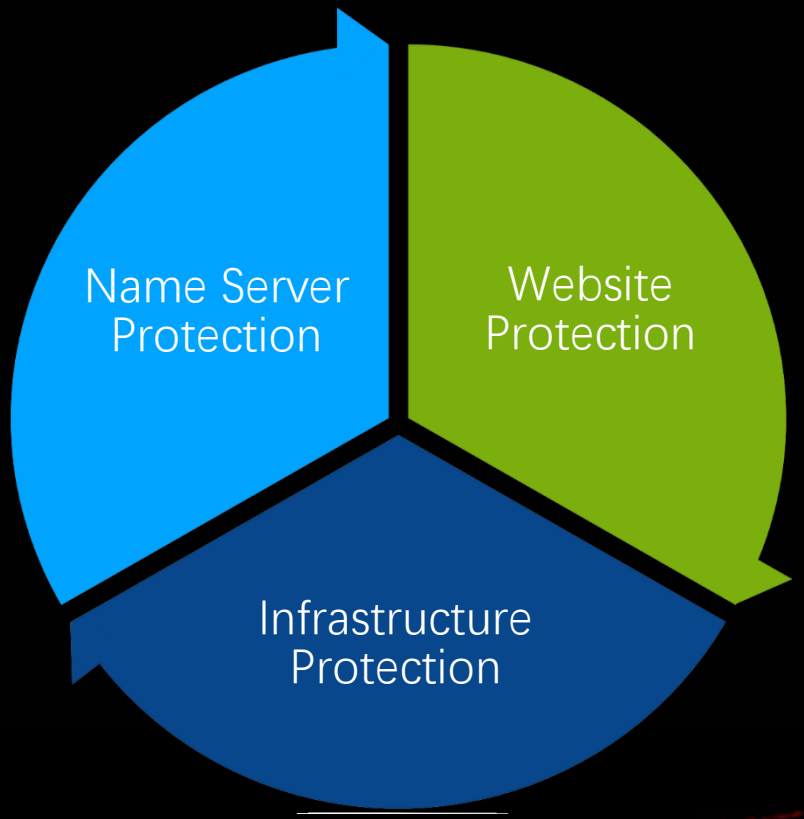
访问控制
拦截特定IP、区域与国家的访问

机器人攻击迁移
拦截自动化攻击，恶意机器人、蜘蛛与垃圾散播者

WAF
拦截黑客攻击
OWASP Top 10 attacks (SQLi, XSS, etc.)

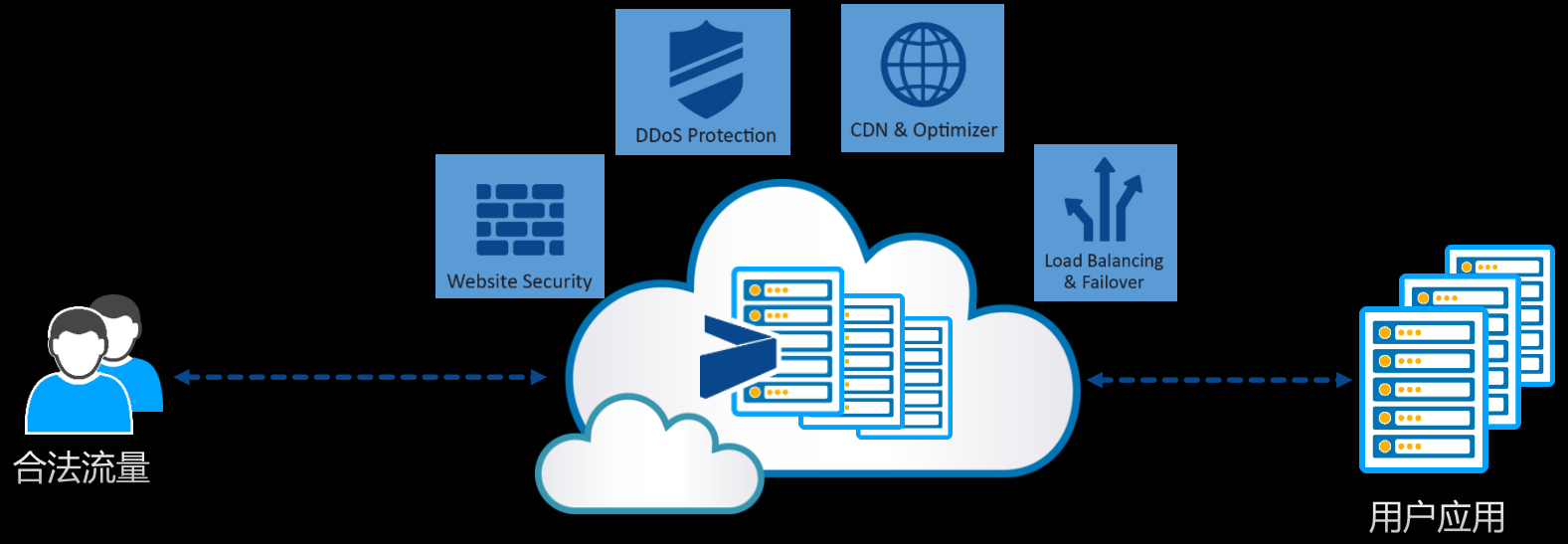
规则策略定制引擎
防御特殊的攻击

层次化 DDoS 攻击保护



- WEB
- SSH, FTP, Telnet
- SIP
- SMTP
- UDP, TCP
- DNS

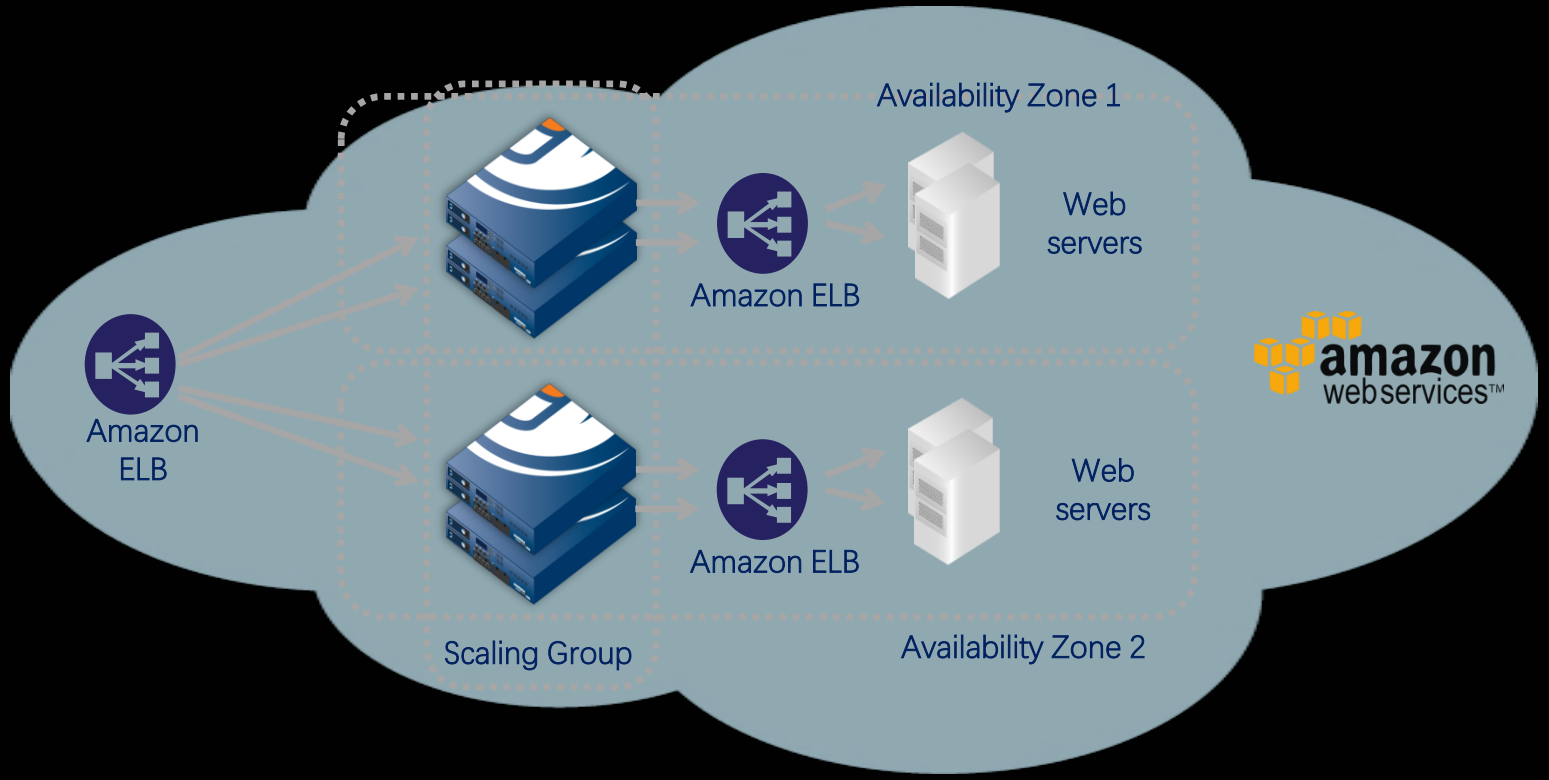
Confidential



通过将WEB应用访问流量路由到Incapsula安全服务网络，恶意流量被拦截，合法流量得到加速

Confidential

SecureSphere WEB应用防火墙与AWS集成



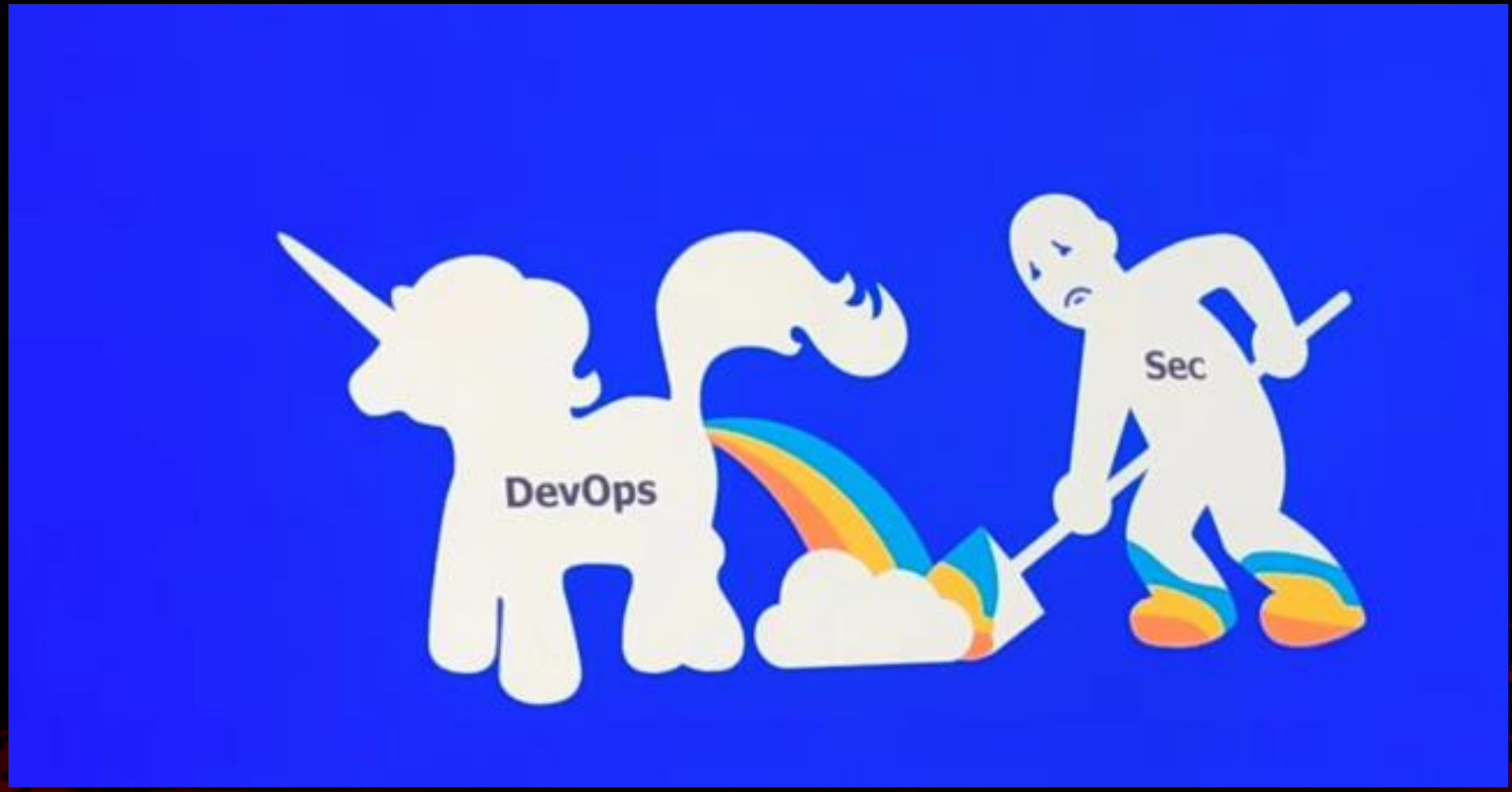
功能

- 全功能的WAF产品
- 与AWS环境紧密集成
  - 快捷部署
  - 灵活伸缩

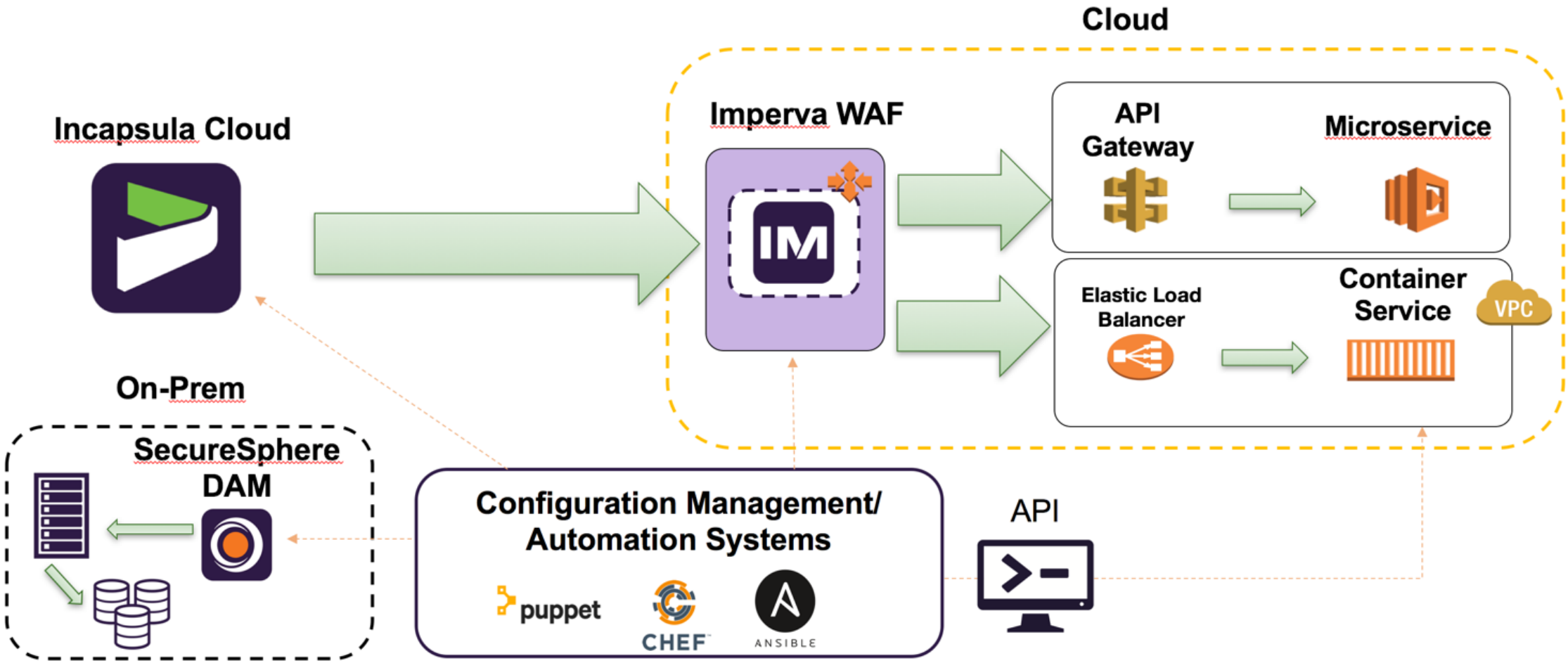
优势

- 减少部署时间
- 降低网络复杂性
- 按需付费（无需购买、维护硬件）

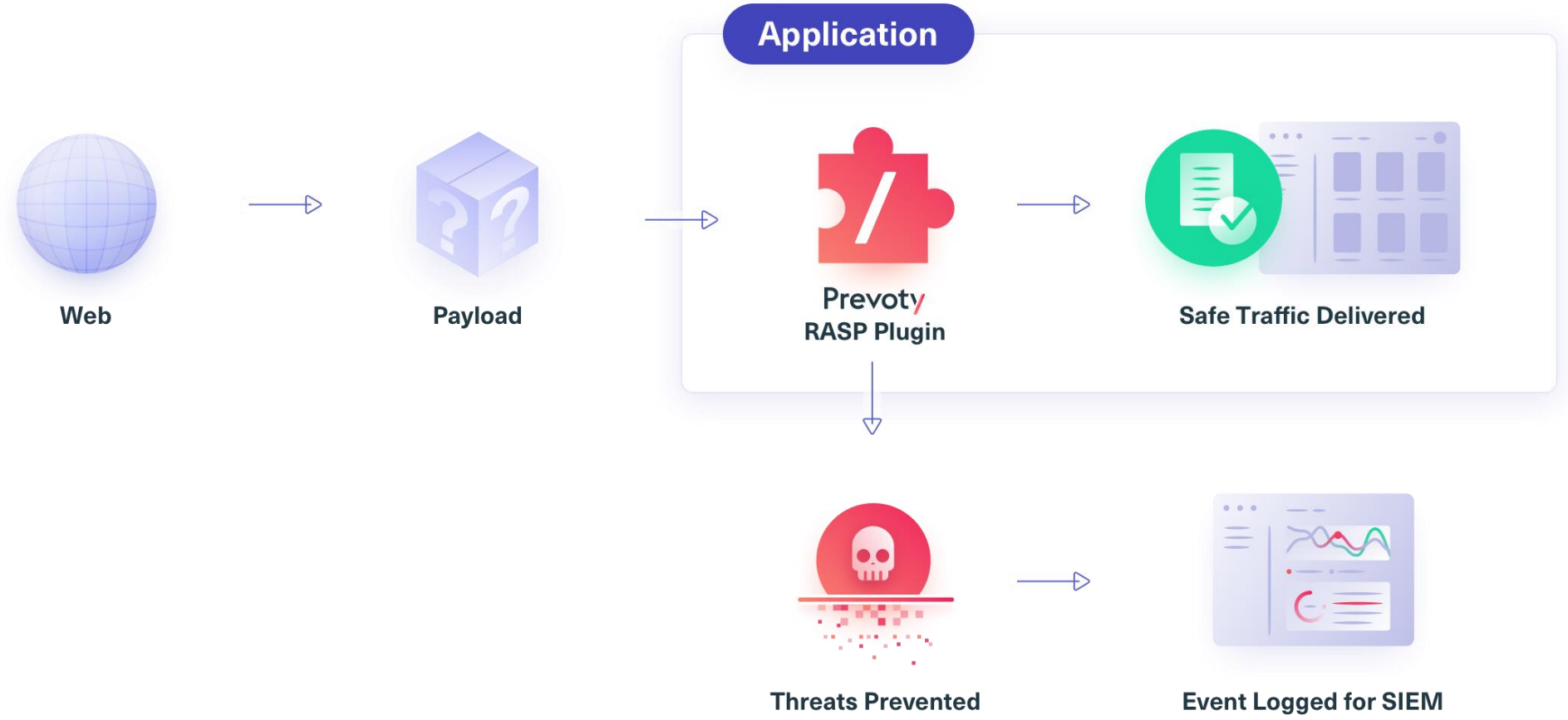
云端DevOps运行环境安全防护

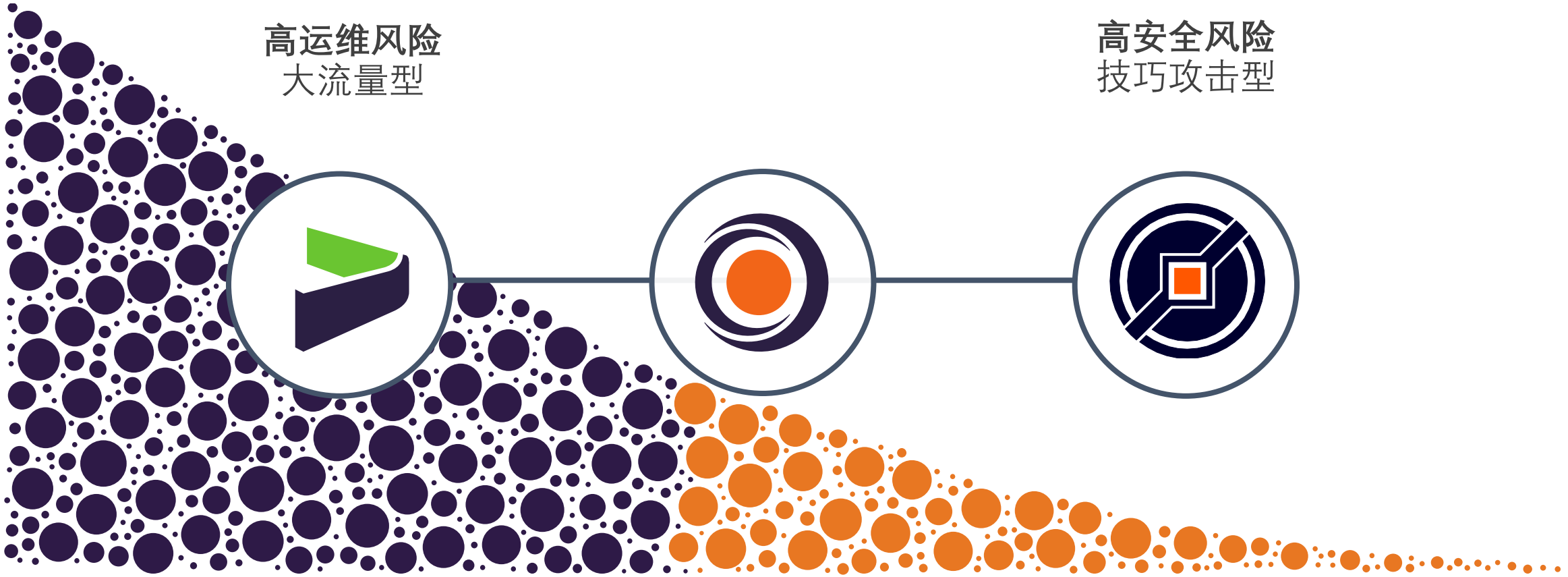


云端DevOps运行环境安全防护



RASP
(Runtime Application Self-Protection)

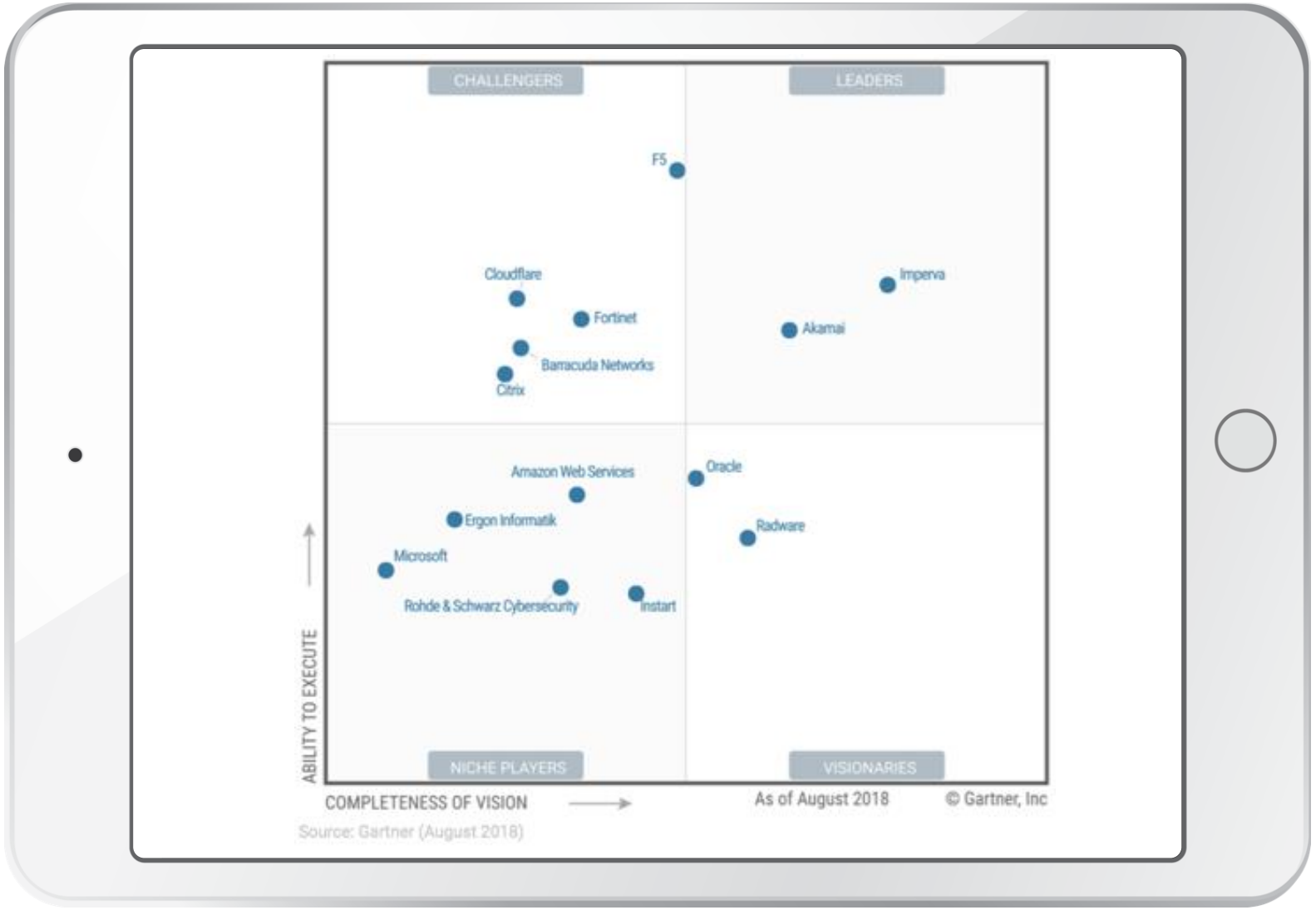




DDoS | 信誉和机器人 | 通用攻击 | 业务层访问控制 | 逻辑攻击 | 应用模型 | 定向攻击

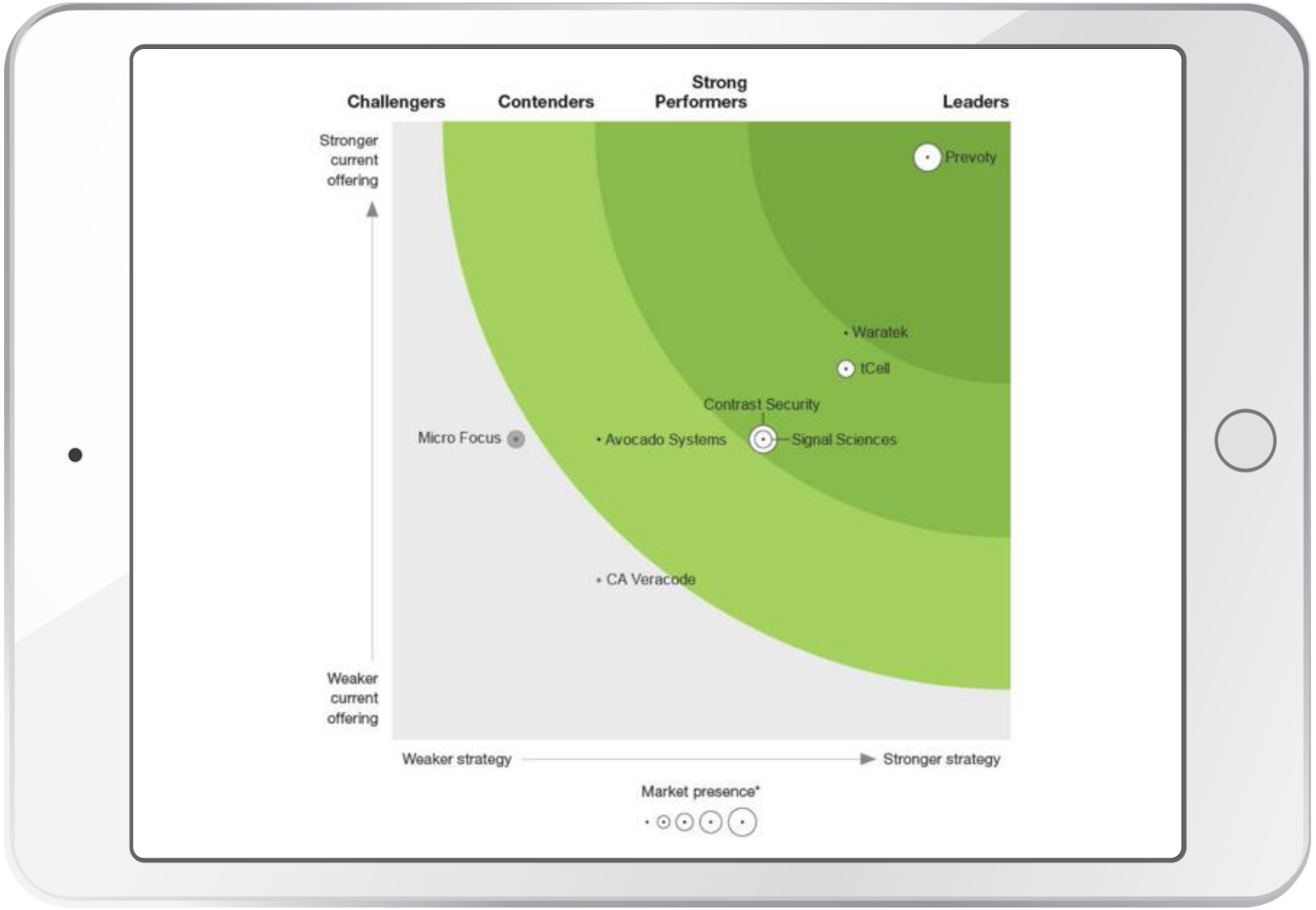
© 2016 Imperva, Inc. All rights reserved.
Confidential
IMPERVA®

2018 Gartner Magic Quadrant for Web Application Firewalls



2018 Forrester New Wave

Rue time application Self-Portection



保护云中的数据安全

Confidential

Imperva Data Protection Product Portfolio

SecureSphere

- 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

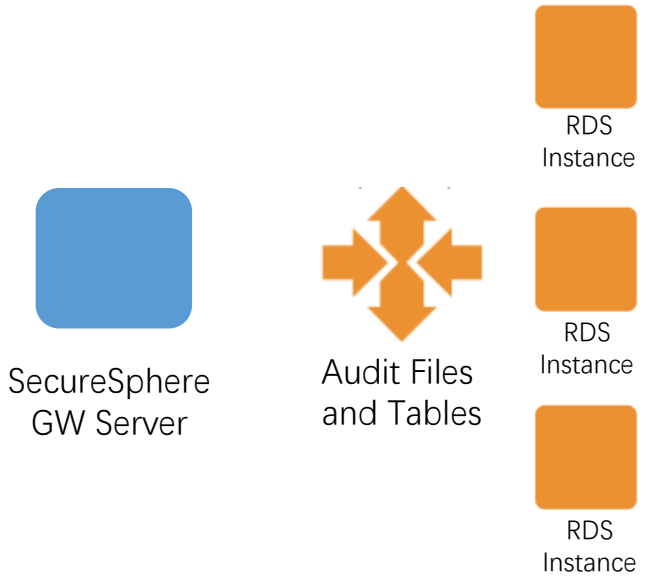
- 基于无监管机器学习的用户行为分析解决方案
- 零安全策略设置
- 自动化侦测各种异常的数据访问行为

Camouflage

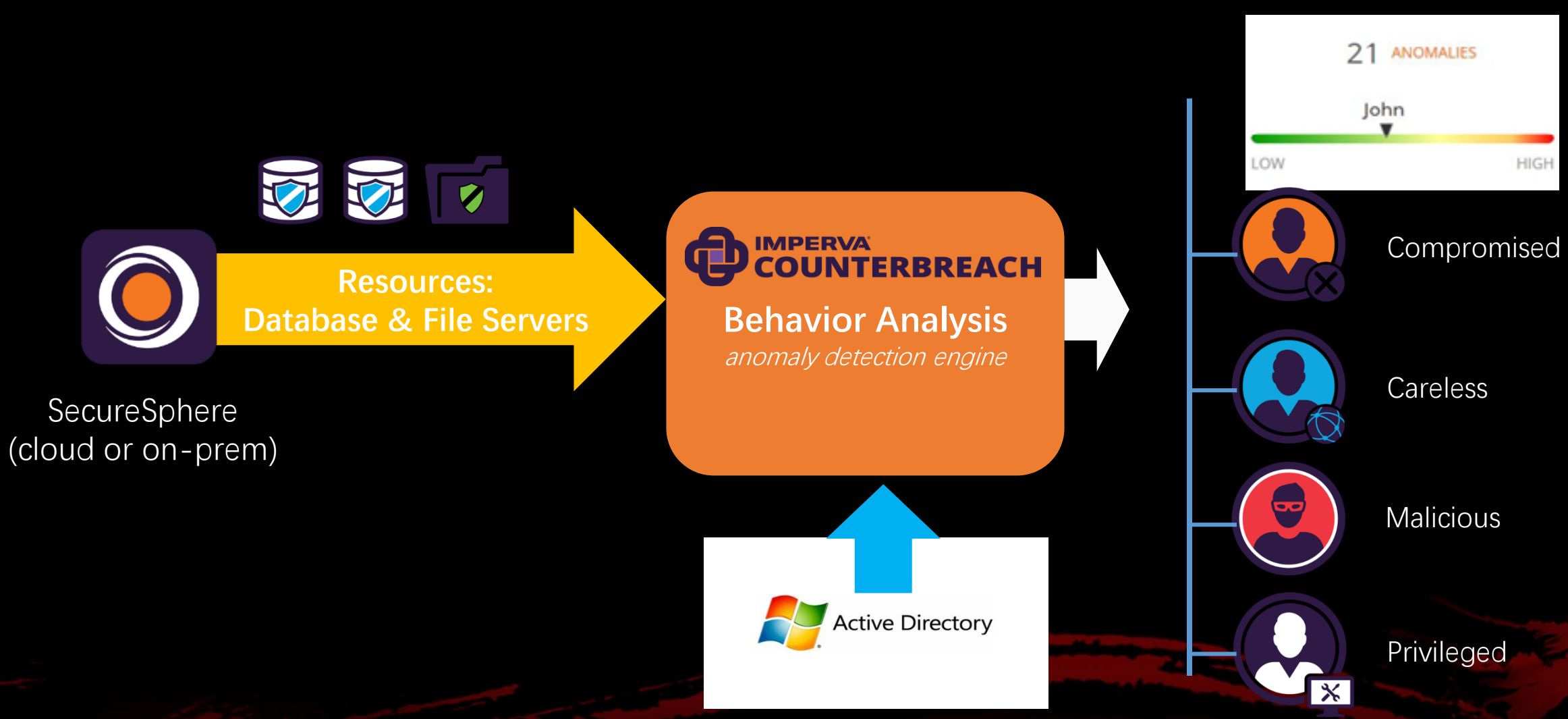
- 数据脱敏解决方案
- 使用接近真实的伪造数据替代敏感数据
- 避免敏感数据被非生产系统使用

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



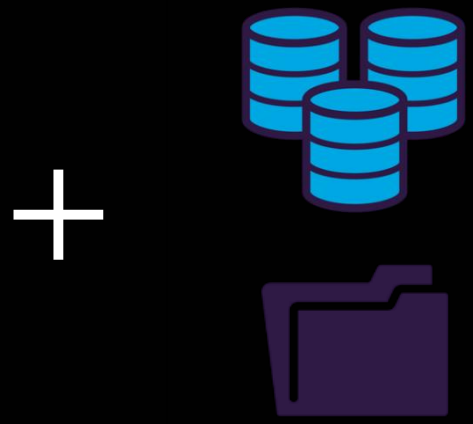
CounterBreach方案仍然可以应用到云端环境中



利用CounterBreach发现云端数据的滥用

访问者分类	Application 	or	Interactive User 
数据库账号分类	Service Account 	or	Personal DB Account 
数据表分类	Metadata 	or	Business Critical Data 
数据库分类	Transaction Processing 	or	Data Warehouse 

不间断的数据访问检测



利用数据掩码确保迁移到云端各种环境中的数据安全

MAP
敏感
数据格局

ORACLE

Microsoft SQL Server

IBM DB2

TERADATA

SYBASE

Windows

vmware

Linux

REMOVE
删除敏感信息的数据

ACCELERATE
数据交付的过程使用更多的
副本，风险较小

DEV & TEST

DATA ANALYTICS

COMPLIANCE

CLOUD

General Data Protection Regulation

HIPAA Compliant

FERPA compliant

PCI DSS COMPLIANT

OUTSOURCING

AND MORE

DISCOVER

PROTECT

COMPLY

THANK YOU