现代数据库环境下的安全思考

现代数据库环境下的挑战

安全覆盖

针对 DBaaS 环境
针对定制化数据库平台
针对混合部署环境

价值

输出有价值的报告、
视图、分析

成本

管理和运维成本
其他资源成本

合规高要求

超大数据检索、查询、存储
信息补充

如何覆盖更多现代数据库安全需求

覆盖更多的现代数据库形态

流量分析的方法可能无法覆盖所有现代数据形态，利用原生日志来做补充

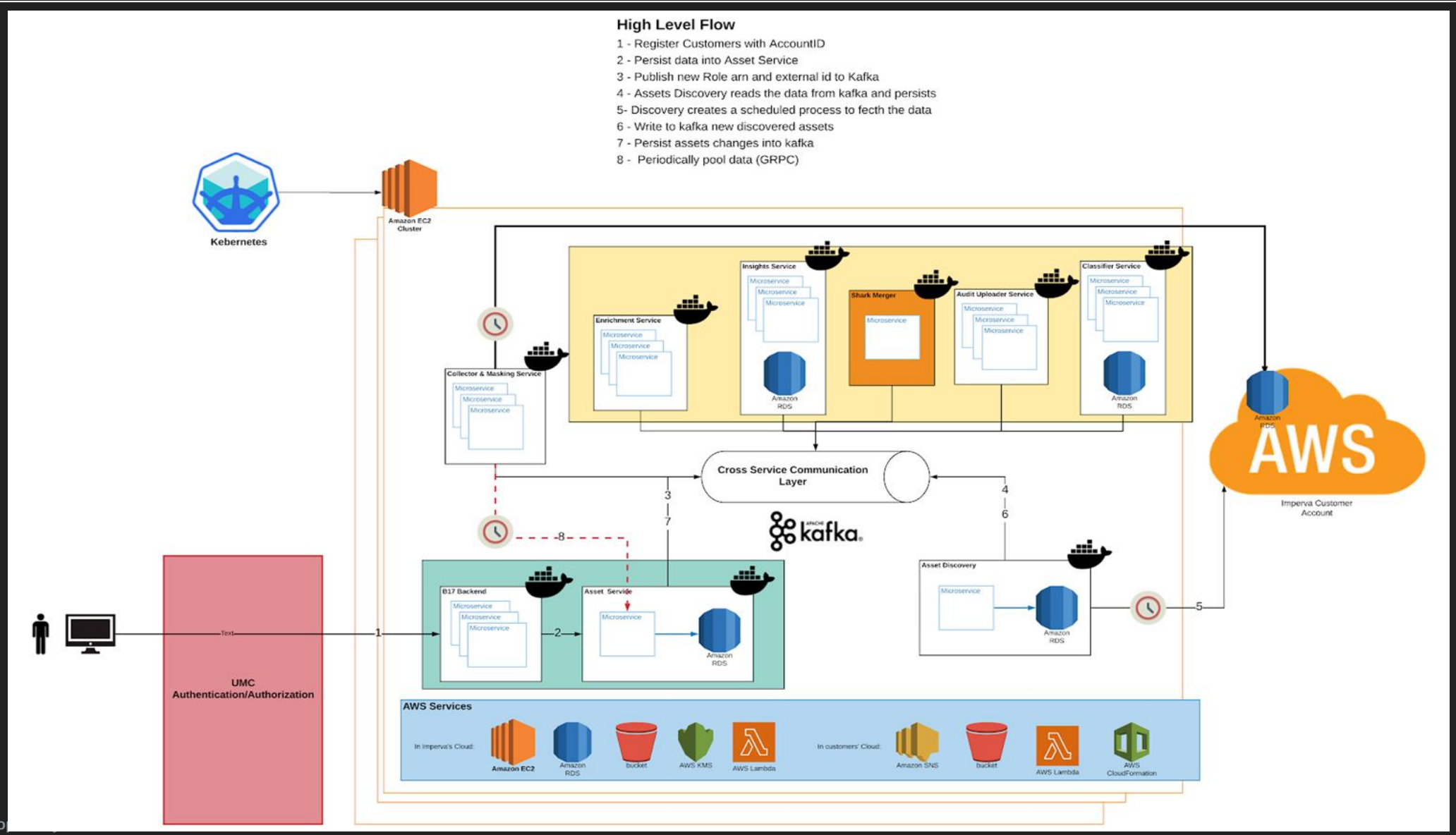
DBasS的全面覆盖

云端的数据安全是未来的焦点，新手段和新技术的涌现

补充完整信息

CMDB、VA、IAM等相关信息的补全

Cloud Database Security 创新技术



imperva

如何进行超大数据的存储和检索

Table

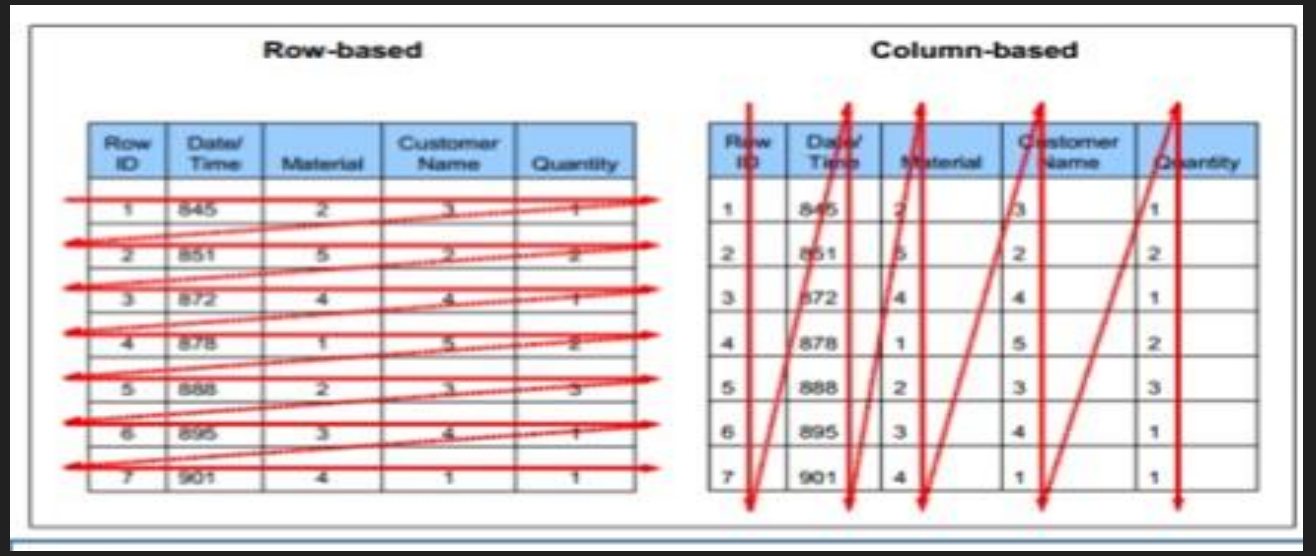
	Country	Product	Sales
Row 1	India	Chocolate	1000
Row 2	India	Ice-cream	2000
Row 3	Germany	Chocolate	4000
Row 4	US	Noodle	500

Row Store

Row 1	India
	Chocolate
	1000
Row 2	India
	Ice-cream
	2000
Row 3	Germany
	Chocolate
	4000
Row 4	US
	Noodle
	500

Column Store

Country	India
	India
	Germany
	US
Product	Chocolate
	Ice-cream
	Chocolate
	Noodle
Sales	1000
	2000
	4000
	500



行存储 vs 列存储

怎样让安全数据有价值和降低成本?

提供风险分析智能

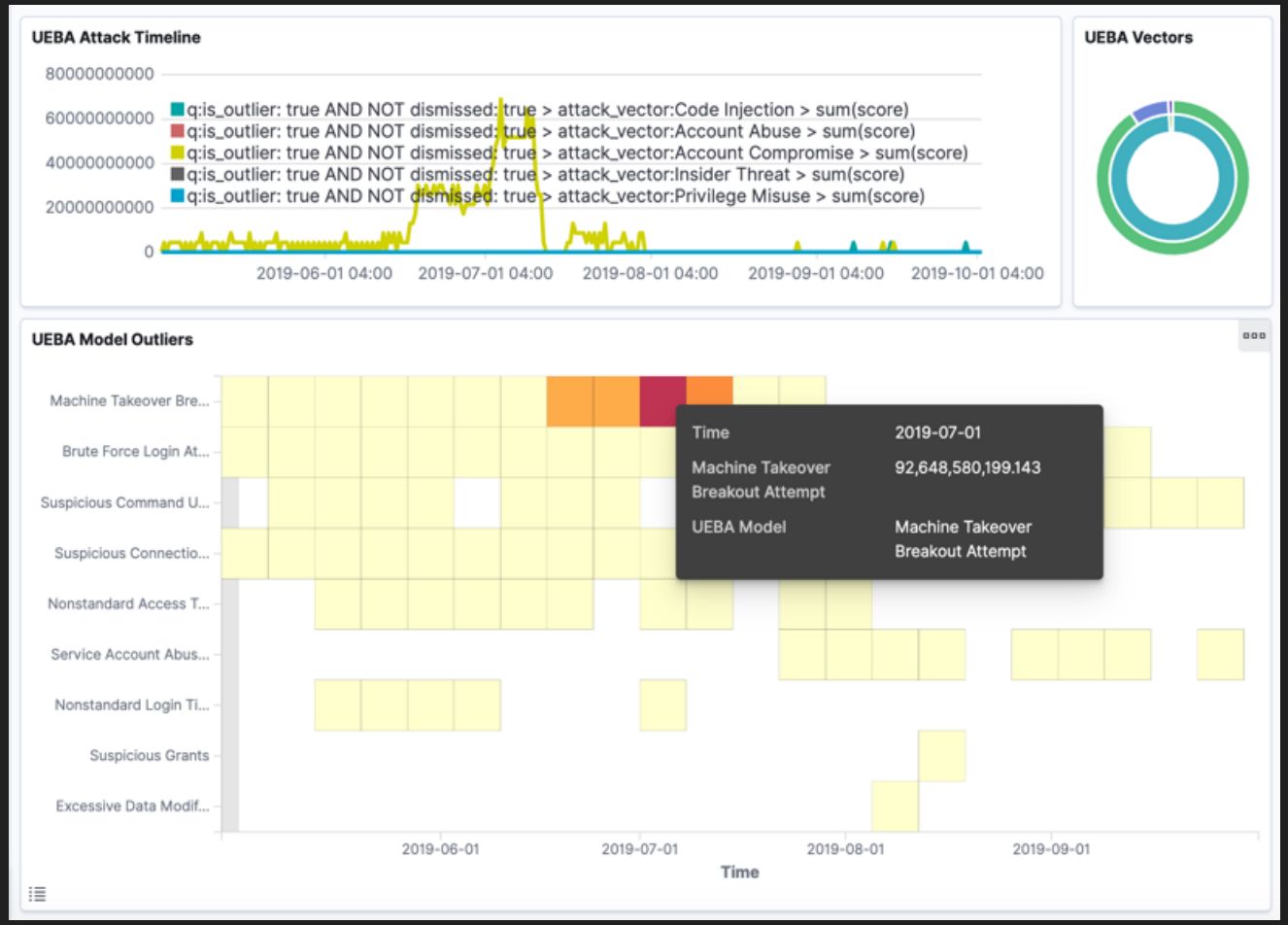
利用无监督学习的UEBA机制，将原始的审计数据变成有价值的风险分析信息

安全数据服务化

为各种团队提供安全数据服务，提供全面、完整和统一的数据库安全相关的数据

自动化编排和响应

除了数据存储和处理成本之外，安全运维成本是巨大的开销，自动化运维势在必行

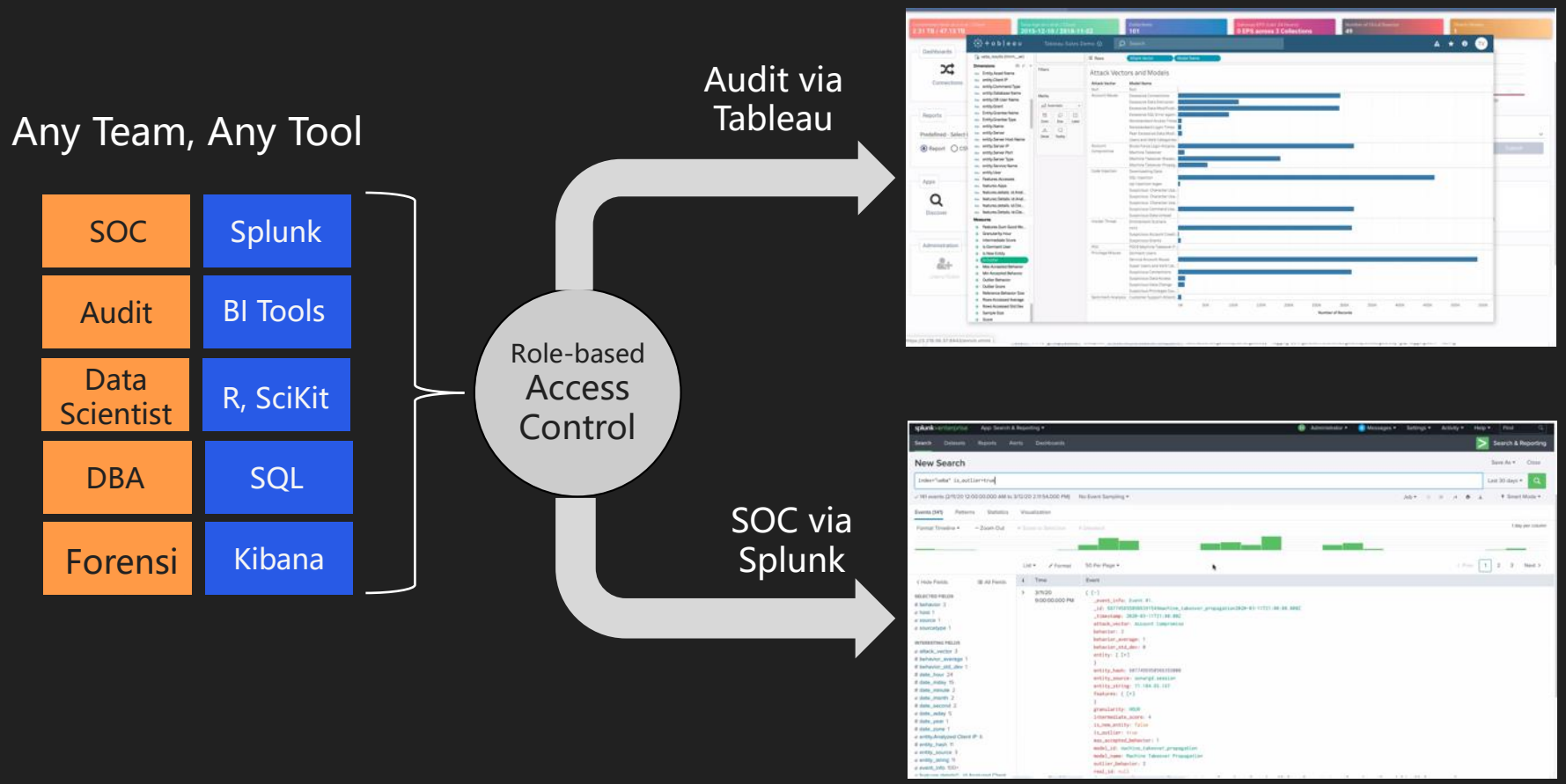


imperva

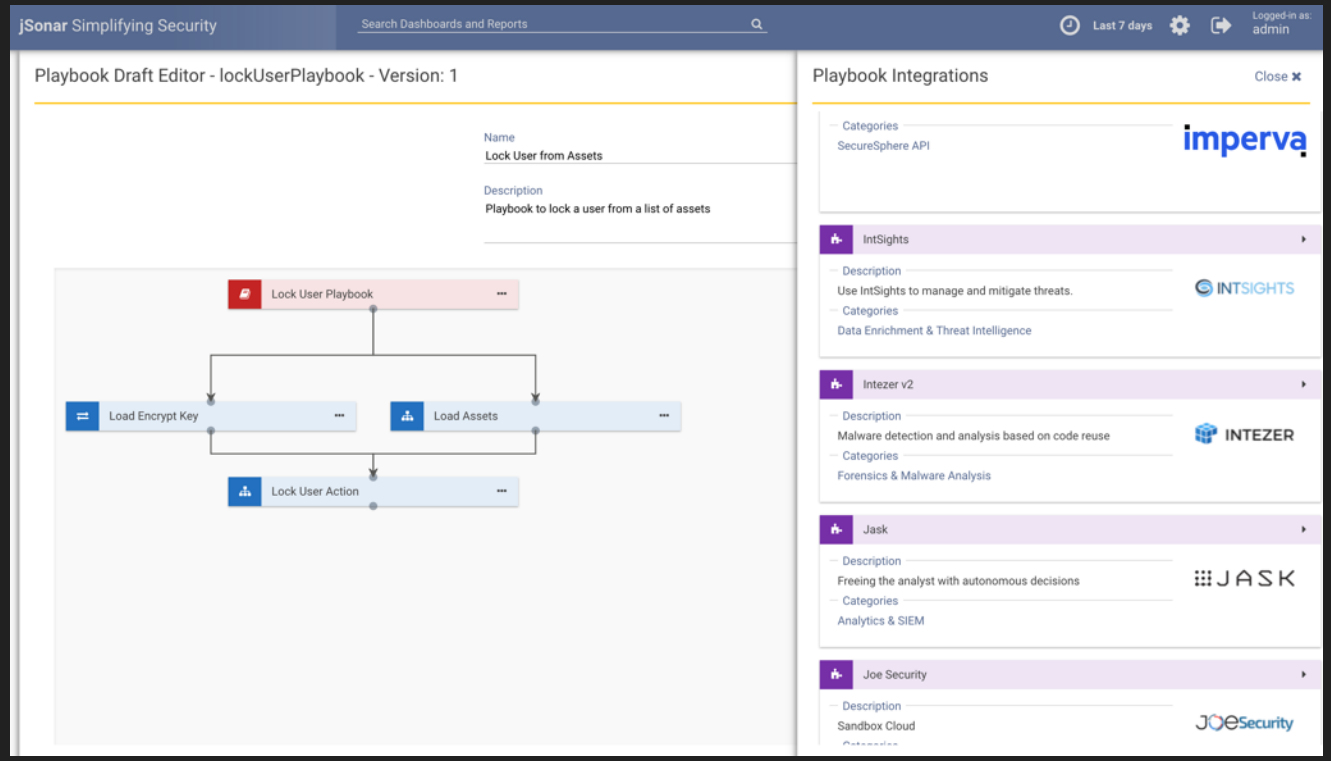
针对数据安全的UEBA

用户	User identity Client IP Server IP Client app	User identity User department	User identity Client IP Server IP Client app	User identity Client IP Server IP Client app	User identity User department
数据	Database name Table name Data sensitivity Schema SQL operation SQL operation Type	Database name Data sensitivity Table name Schema Number of rows SQL operation	Database name Table name SQL operation SQL operation type	Database name SQL operation SQL operation type Query	File operation File path File name File type File share name
风险场景	↓ **可疑应用数据访问**	↓ **数据库记录访问过多**	↓ **服务滥用**	↓ **可疑动态SQL 活动**	↓ **可疑文件访问**

让安全数据服务化



数据库安全自动化编排和响应



数据库安全SOAR

建立以数据库为中心的自动化和响应平台

- 基于UEBA的分析结果来进行下一步的行动
- 避免大量的重复数据处理工作
- 定制数据安全Playbook

数据库安全中台?

统一数据接口
避免“重复造轮子”

获取数据效率低、质量差
避免“烟囱式立项”

挖掘数据的价值
数据服务化

数据拥有成本
增长过快

企业级数据库安全服务平台

现代企业数据库安全智能平台

数据展现

- 互动式数据探索
- 统一企业视图
- 数据处理流程自动化
- 多年数据保存
- 自助报告
- SOC优化

数据智能

- 统一数据模型
- 数据富集与关联
- 数据风险分析
- 可扩展UEBA
- 数据SOAR

通用采集

数据采集

扫描结果

- 发现
- 漏洞评估
- 分类
- 用户权限管理

活动监测源

- 代理监控
- 无代理监控
- 云
- DAM解决方案

其他数据源

- 上下文元数据
  (IAM、变更控制、CMDB等等)
- 任何工具
  (Qualys、Tenable、Varonis等等)

imperva

Thank You!