你**改变**世界 我**守护**安全

You **change** the world, we **secure** it.

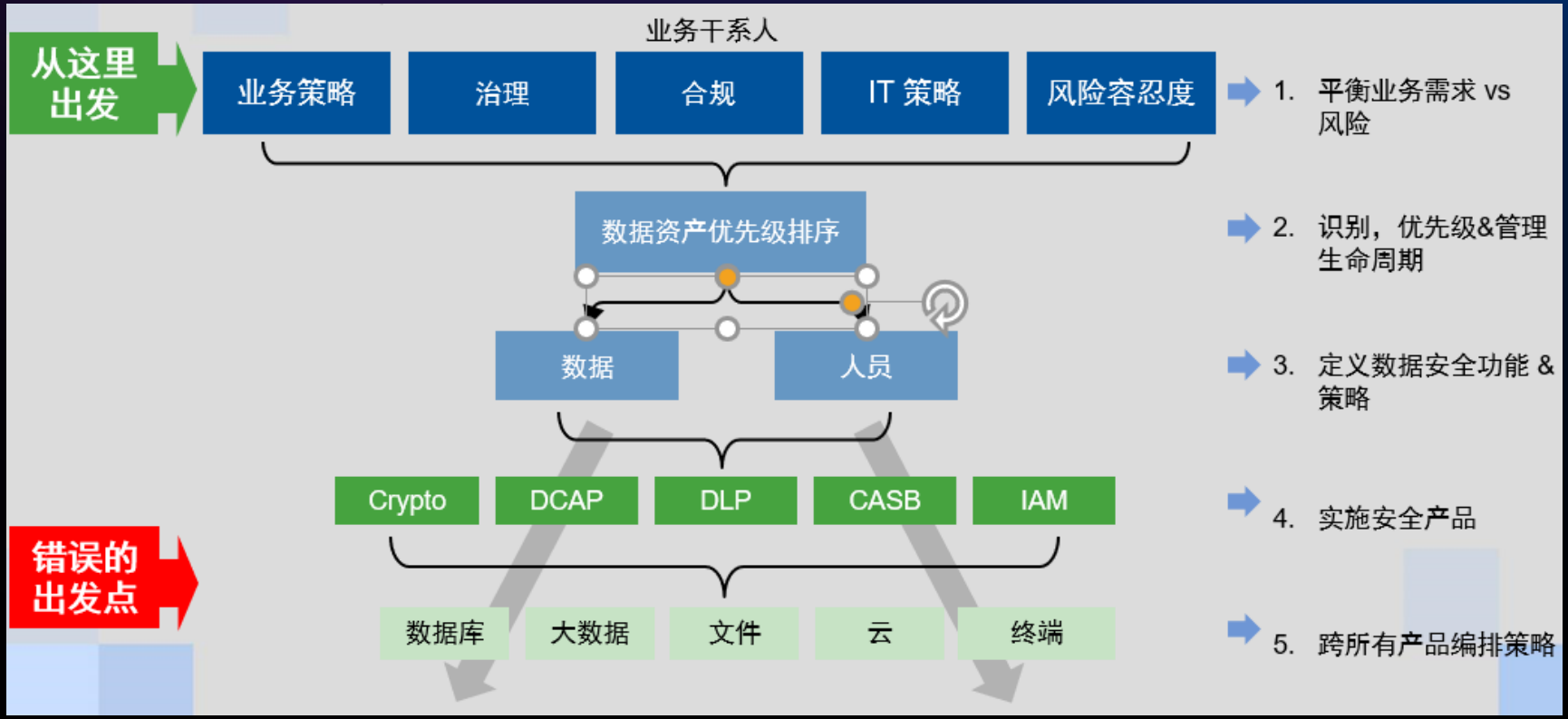
2019 IBM 企业安全峰会

数据库保护Guardium与特权账号管理Secret Server，敏感数据保护的两把双刃剑

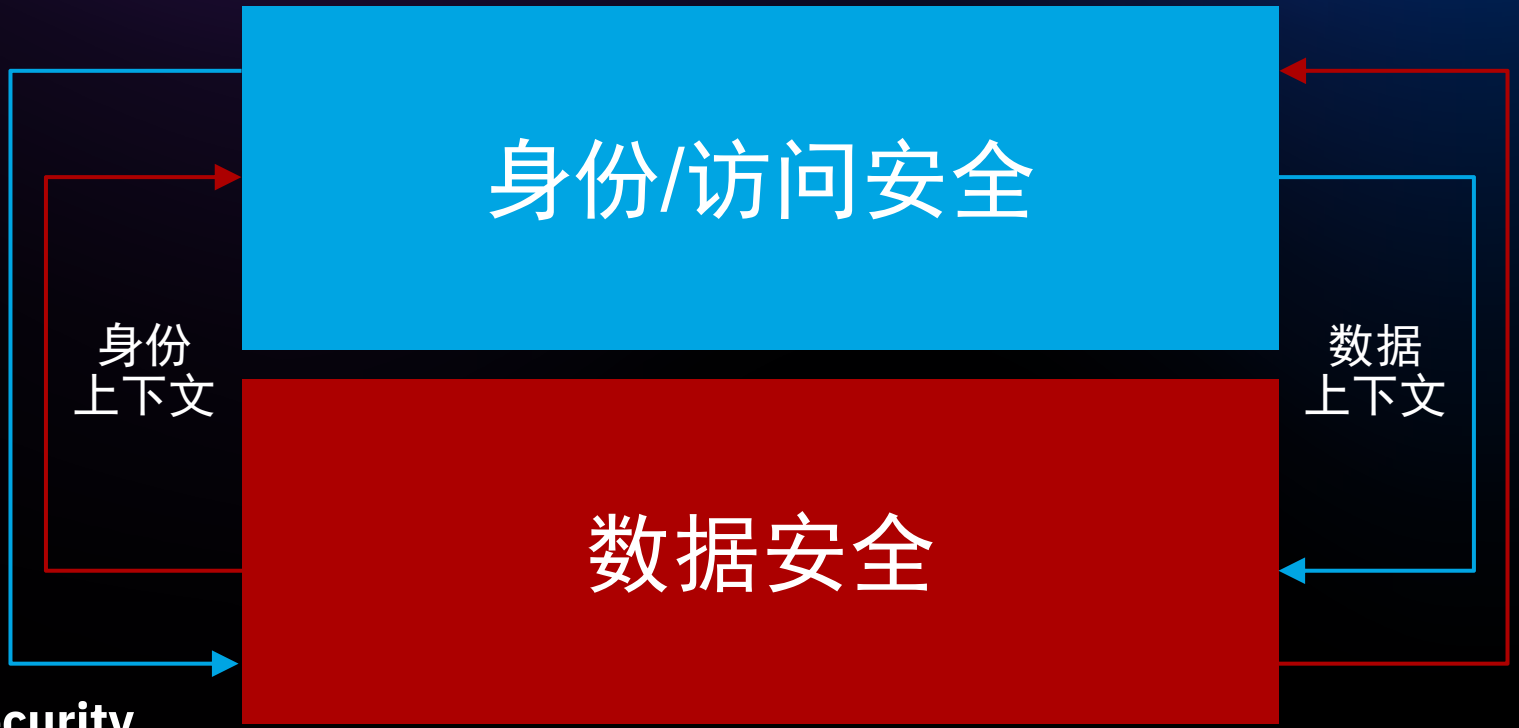
高 爽

IBM大中华区安全事业部数据安全架构师

符合企业环境的数据安全架构



身份安全与数据安全的融合



市场上存在哪些问题？

- **80%** 的安全问题涉及特权凭证[1]
- **54%** 的公司，在今天，使用纸张或者Excel管理特权凭证[2]
- **$3.62 million**
  全球平均数据泄露成本[3]

[1] The Forrester Wave: Privileged Identity Management, Q3 2016
[2] Dimensional Research Global PAM Survey 2017
[3] 2017 Ponemon Cost of a Data Breach Study

今天，存在哪些风险？

- 未知的和未被纳管的特权凭证
- 特权凭据由IT管理员共享
- 密码和SSH密钥是静态的
- 未强制执行多重身份验证
- 特权访问级别过高
- 缺乏应用程序控制

下一代特权账户管理主要使用场景

减少
数据泄露

发现
未知特权账号

定义安全加密的
密钥保险库

监控
特权账号的使用

遵从
法规和满足审计需求

保护系统
当管理员离职时

管理
服务账号

在**DevOps**过程中，保护特权账号

打破
玻璃杯（零信任）

IBM Security Secret Server

轻松检测，管理和审核特权帐户和身份验证机密，如密码和SSH密钥。

限制用户本地权限以防止恶意应用程序渗透到环境中。

发现

管理 & 审计

监控 & 控制

安全 & 保护

IBM Security Secret Server

发现

- 在您的IT环境中发现以前未知的特权帐户
- 可轻松保护和管理新的特权帐户
- 引入持续流程以保持对特权访问的控制

发现

管理 & 审计

监控 & 控制

安全 & 保护

IBM Security Secret Server

管理 & 审计

- 建立用于获取特权访问的工作流程
- 通过签入和签出功能将密码和SSH密钥安全地存储在保险库中
- 自动轮转或更改密码和SSH密钥
- 对活动进行全面的审计跟踪，以创建报告并证明合规性

发现

管理 & 审计

监控 & 控制

安全 & 保护

IBM Security Secret Server

监控 & 控制

- 准确了解您的特权帐户的使用时间，方式和原因
- 通过限制业务和IT用户的权限来提高端点安全性
- 停止端点上的恶意软件

发现

管理 & 审计

监控 & 控制

安全 & 保护

IBM Security Secret Server

安全 & 保护

- 防止未经授权使用特权帐户
- 记录和监视特权会话活动以进行审计和取证
- 在端点上实施最小权限策略
- 定义/实施策略以控制端点用户的本地权限

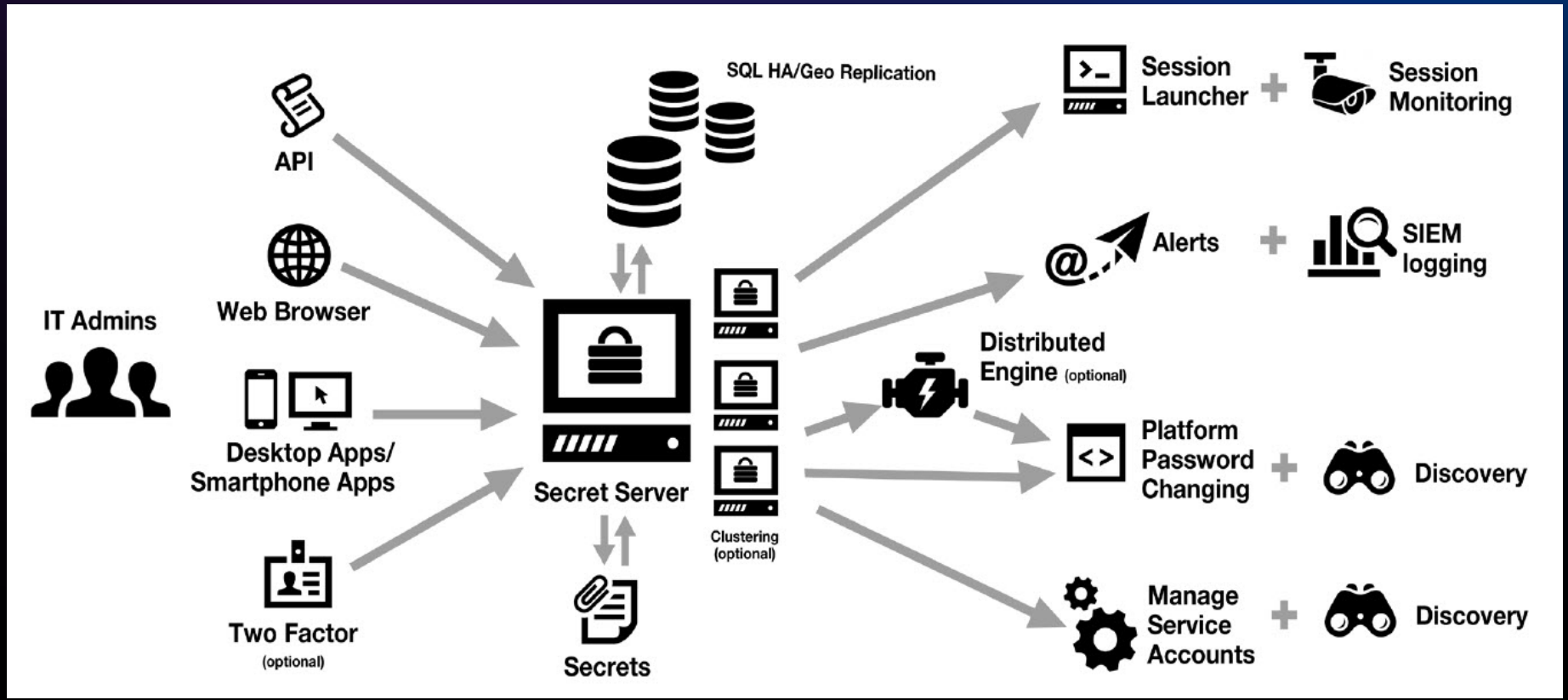
发现

管理 & 审计

监控 & 控制

安全 & 保护

IBM Security Secret Server 逻辑架构



DEMO-1

数据安全技术架构


安全运维与响应
生态圈
DLP
应用安全
身份和访问管理
信息安全 & 风险管理
Data Risk Manager
Guardium Big Data Intelligence
风险管理
漏洞评估
行为分析
Guardium Analyzer
Guardium Vulnerability Assessment
以数据为中心的审计 & 保护
Guardium Data Protection
合规报告
数据发现
数据分类
活动监控
信息安全执行
Guardium Data Encryption, Multi-Cloud Data Encryption, Security Key Lifecycle Manager
加密
令牌化
脱敏
访问控制
数据库
大数据
数据湖
文件 (系统)
物联网，移动
SaaS
On-Premise, 以

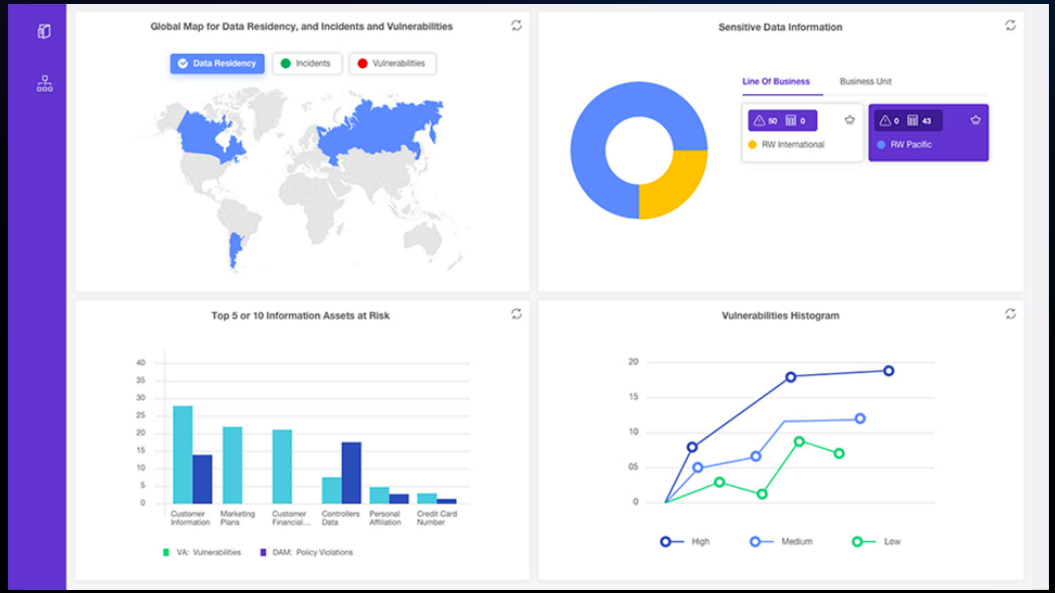
IBM Security Data Risk Manager

识别 – 可视 – 沟通

Data Risk Manager 为管理人员及其团队提供业务可理解的数据风险控制中心，帮助发现，分析和可视化与数据相关的业务风险，以便他们能够有效地协作并采取措施保护其业务。

主要收益：

- **识别高价值，对业务敏感的信息资产，**并通过交互式数据风险控制中心提供与皇冠明珠数据相关的业务元数据的端到端视图
- **通过业务风险评估建模的方法对潜在风险进行可视化，**该建模将信息资产中的威胁，漏洞，控制和业务属性相关联，以突出显示处于风险中业务并提供补救建议
- 通过易于理解的仪表板和报告，将团队，业务部门和技术之间的数据风险信息**传达给高管**

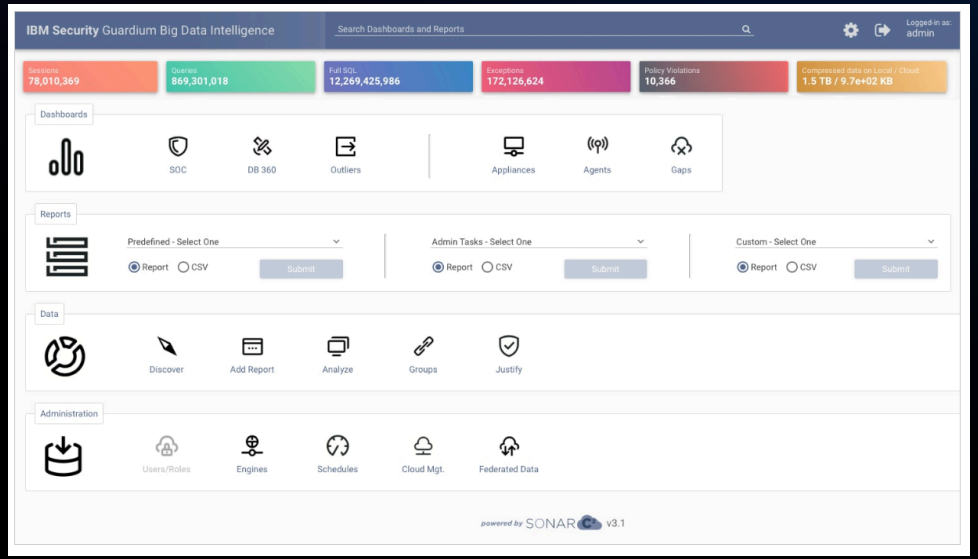


IBM **Security**

IBM Security Guardium Big Data Intelligence

敏捷 - 保留 – 洞察

Guardium Big Data Intelligence 增强您现有的数据安全解决方案，丰富它，能够快速创建优化的安全数据湖，在长时间内保留大量历史数据，以提供新的，丰富的分析洞察力，同时降低成本并提供近实时报告。



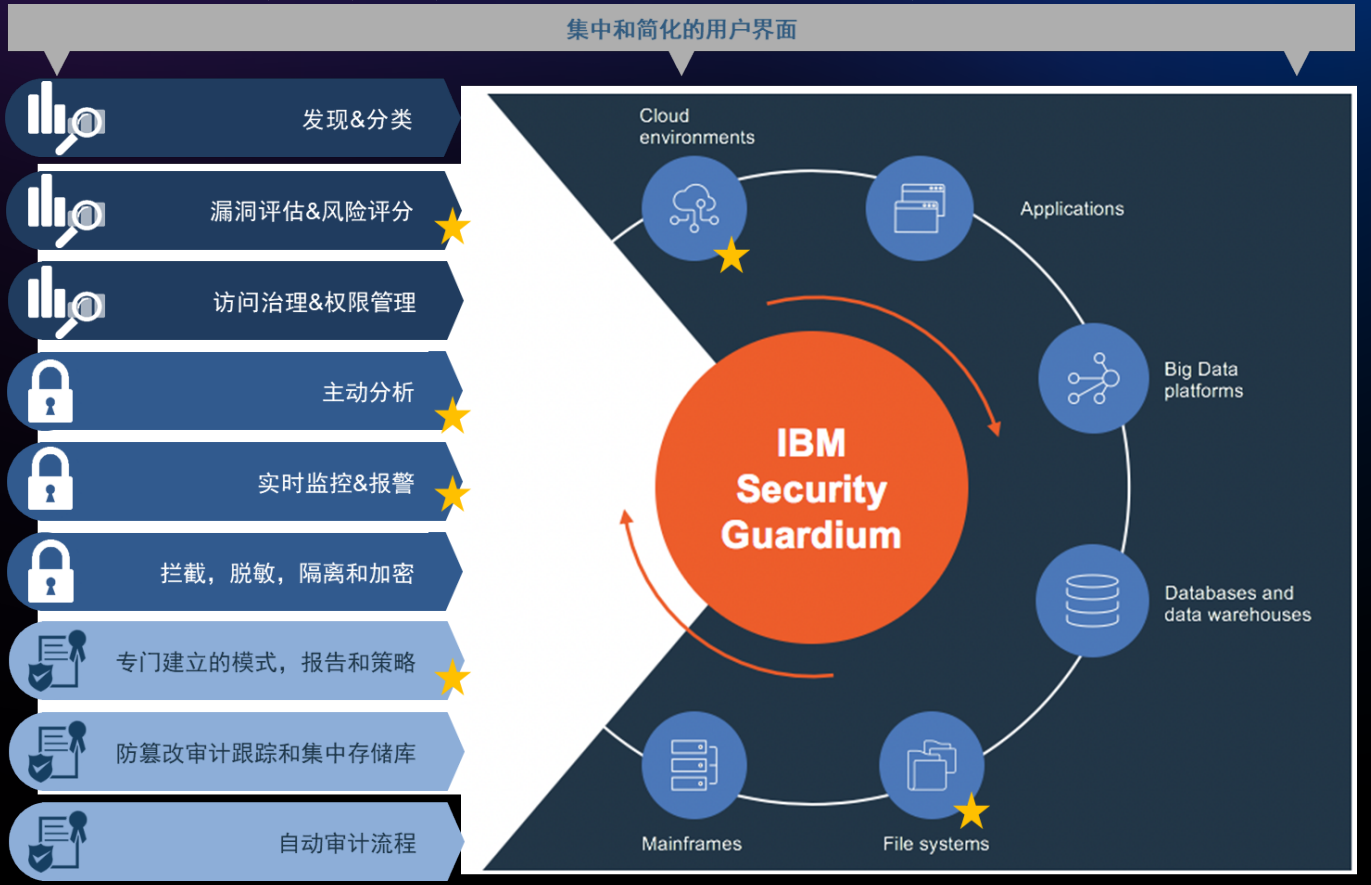
主要收益：

- 通过优化数据安全架构，降低成本和加快部署，**提高数据安全解决方案的灵活性**，同时为用户提供直接，安全的访问和自助报告
- 通过低成本，多年的大数据湖，在不影响性能的情况下，通过在更长的时间范围内存储更多数据，**实现更长的数据保留期**
- 通过大数据安全分析，交互式数据探索功能和灵活的事件级工作流管理器，**提供易于使用的洞察力，以改善数据安全状况**

IBM Security Guardium Data Protection

监控 - 执行 – 遵从

Guardium Data Protection使用自动发现，分类，监控，实时控制和认知分析来保护敏感数据，并简化对预建报告和工作流程的合规性



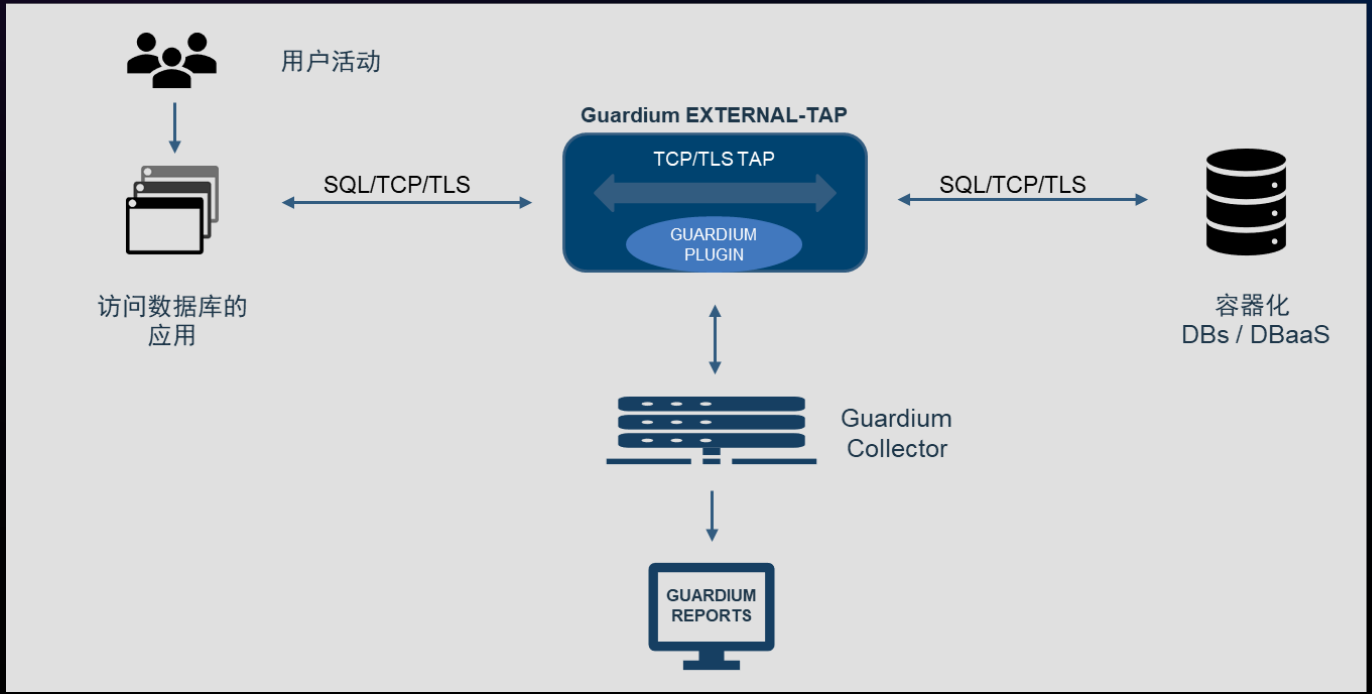
IBM Security

对混合云的支持

DBaaS的新监控功能允许客户端在内部部署和云环境中采用一致的数据保护方法

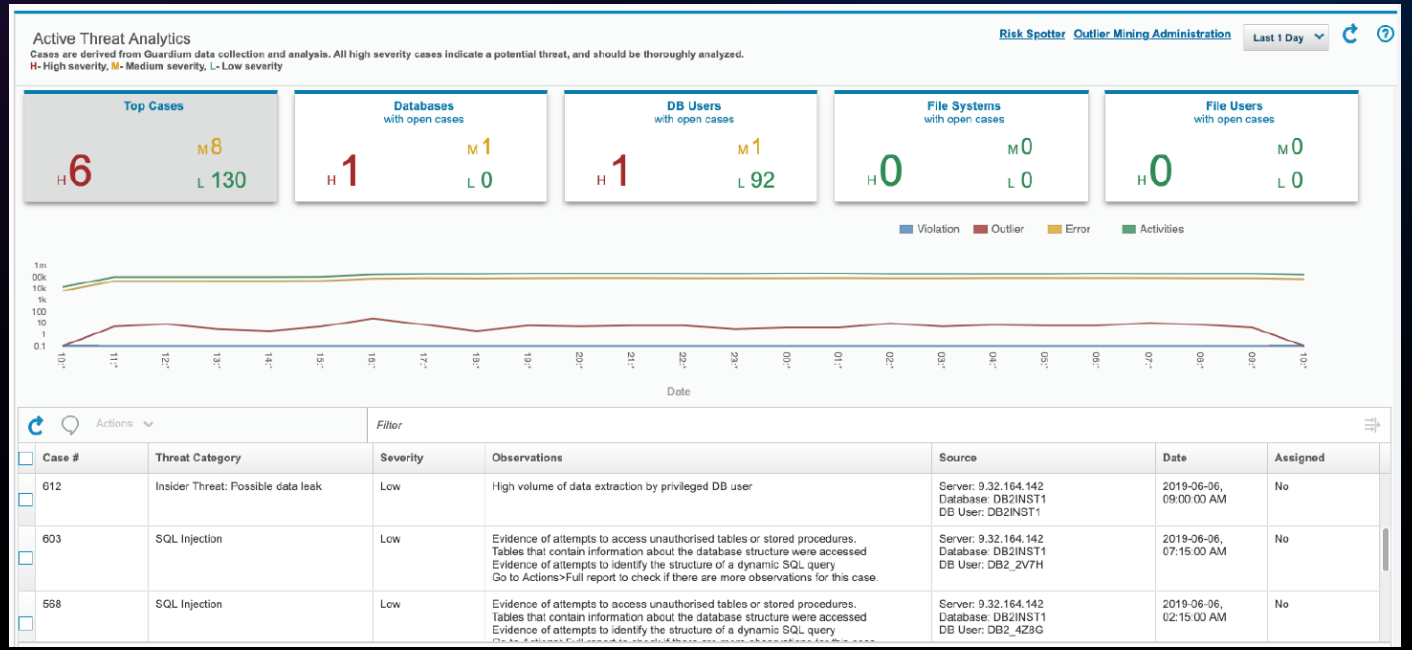
- **新的Guardium EXTERNAL-TAP允许新的和以前不可用的活动可见性级别，以促进更好的保护**
- **支持的平台：AWS RDS（Oracle），Azure MS SQL**

概念架构



主动威胁分析

- SQL注入
- 恶意存储过程
- 数据泄露
- 拒绝服务
- 账户接管
- 篡改Schema
- 篡改数据
- 异常访问



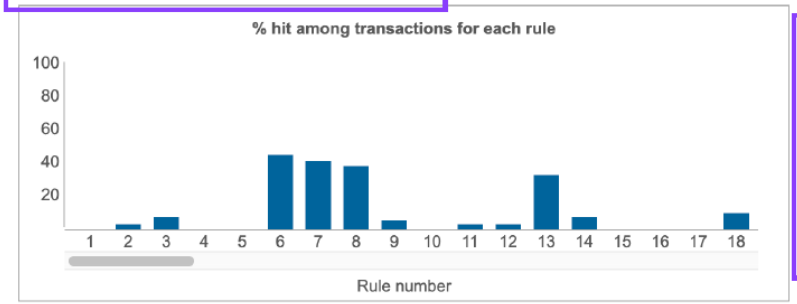
用户风险评估

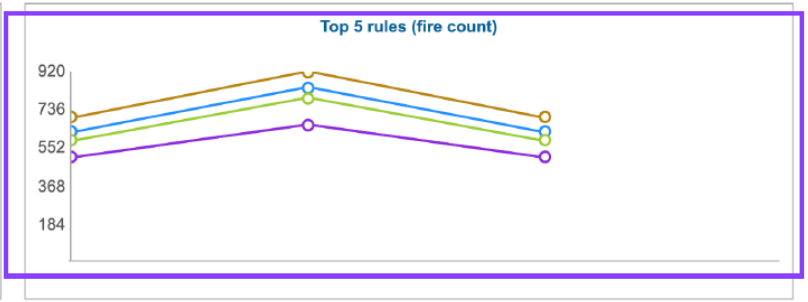
Outliers	The number and severity of anomalies related to the user.
Violations	The number of high and medium severity violations related to the user.
Vulnerability	The number of failed vulnerability assessments for a user.
Sensitive objects	The number of queries on sensitive data related to the user.
Off-work activity	Activity related to the user that occurred in non-work hours.
DDL queries	The relative amount of DDL queries related to the user, out of the total activity.
DML queries	The relative amount of DML queries related to the user, out of the total activity.
Administrative queries	The relative number of administrative queries related to the user, out of the total activity.
Select queries	The relative number of select queries related to the user, out of the total activity.
High volume activity	High volume activities as compared to the average activities of users.

安全策略分析

View continuous analysis results

Time frame: Last 30 Minutes





Details for all policy rules

Download as CSV | *Filter*

Number	Rule	Action	Fire count	% hit among transactions	% hit among rules	Policy
1	Failed Login - GDPR Personal Data - Log Violation by Admin Users	LOG ONLY	0	0	0	Smart Assistant GDPR
2	Failed Login - GDPR Personal Data - Alert if repeated	ALERT PER MATCH	54	3	1	Smart Assistant GDPR
3	SQL Error - GDPR Personal Data - Alert on Risk Indicative errors	ALERT PER MATCH	337	7	1	Smart Assistant GDPR
4	REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details	ALERT PER MATCH,LOG FULL DETAILS	0	0	0	Smart Assistant GDPR

IBM Secret Server + QRadar

IBM Secret Server 发送特权账号相关的事件数据给 QRadar

用户场景

- 深入了解特权帐户的使用（例如Windows本地管理员，服务或应用程序帐户，UNIX root帐户）
- 管理特权帐户中的实时事件，并在其特权帐户管理策略中构建自定义风险分析
- 使用QRadar UBA识别异常或有风险的特权用户行为

收益

满足合规 强制执行SOX，PCI DSS和HIPAA等详细报告，审计和日志

降低风险 通过快速检测内部网络攻击

IBM Secret Server + Guardium Data Protection

Guardium确保IBM Secret Server数据库保险库中的特权访问合规并且安全

用户场景

- 为存储在Secret Vault中的数据添加另一层保护
- 监视和审核Secret Vault中的所有数据活动，包括受保护的保管库中的特权用户（如开发人员或数据库管理员）执行的操作
- 实时实施安全策略，阻止在Secret Vault中执行不需要的操作

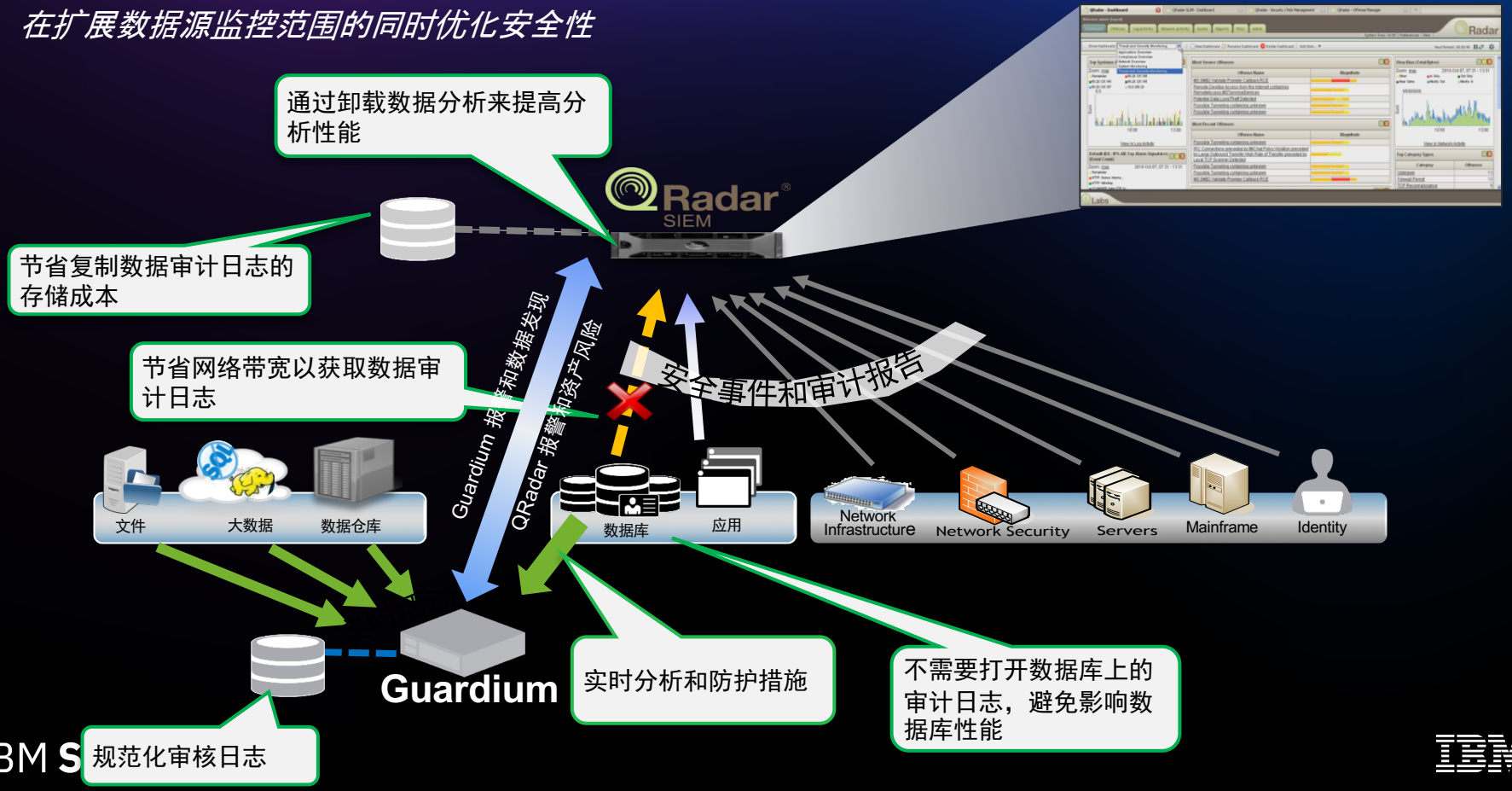
收益

增强安全性 - 通过为存储在Secret Server凭证保险库中的所有数据创建第二层防御

满足合规性 – 通过确保实施策略，阻止不需要的操作以及支持审计员所需职责分离的防篡改数据访问审计跟踪

Guardium Data Protection + QRadar

在扩展数据源监控范围的同时优化安全性



IBM S

IBM

DEMO-2

Thank You