抓特权内鬼，防黑客泄露
避免敏感数据泄露后的巨额损失

客户为何需要关注?

- 国外的某连锁酒店因会员资料泄露，遭判处1.23亿美元的罚款；某航空的数据泄露，更面临2.3亿美元的罚款；国内最近的某快递公司因为员工窃取用户信息，卷入千万诈骗大案。
- “特权账号安全”在Gartner**十大网络安全项目**2018年开始连续两年名列第一。
- **已知**的安全泄漏中，**80%与“特权账号密码”有关**。
- 数据泄露的平均生命周期，**潜伏期206天**，超过一般审计要求的6个月时间。

IBM解决方案优势

混合云时代，面对内部人员泄露和外部攻击等威胁，以合规审计为目的的单一产品是不够的。

企业最宝贵的资产是数据，而绝大部分的数据泄露又都是利用特权账号，所以我们建议”**内外兼修、双重防卫**“，一方面从泄露管道严抓特权账号，另一方面也从源头保护关键敏感数据。在提高抵御恶意攻击免疫力的同时，也证明了责任归属，符合审计原则。

特权账号管理 IBM Security Secret Server + 数据安全防护 IBM Security Guardium

- 纵观国内外，IBM是少数在这些领域都提供解决方案的厂商。
- 在Forrester报告中，Guardium 和 Secret Server 都居于“领先”地位。
- IBM是全球排名第一的企业级安全厂商，特别着重导入AI以应付新的未知威胁。
- 可以和IBM其他安全产品无缝整合，例如与QRadar整合，将账号和数据库的异常行为响应到SIEM平台，并因此做出紧急处置。
- 特权账号管理系统安装容易，不需要专业服务来配置和管理，迅速见效；有严格的本地特权账号管理和更完整的审计报表，另外针对数据库本机流量和云上数据，能做到完整监控。

对客户的效益价值定位

- 减少数据泄露的风险与成本 –建立严格的双保险机制，透过特权账号密码保护机制，减少有意和无心的特权账号密码泄露风险，保护“通往王国的钥匙”，同时分析并找出敏感数据，并进而监视数据源的用户活动，达到保护“皇冠上的明珠”

- 合规性及风险控制 – 完整的审计报表，达到GDPR和等保2.0等对于审计管理的要求；同时更可以在万一数据泄露发生时，尽速抑制泄露，做好风险控制。

客户该怎么做

第一步：联系IBM，安排Secret Server 及 Guardium 的 POC，搜索特权账号，进行数据库扫描，发现错误配置、弱密码、权限过高等漏洞，以及是否有违规构建的数据库。

第二步：项目实施，进行清理、分类、管理、监控，控制数据泄露风险。

第三步：定期扫描清理，做好特权账号生命周期管理，保护关键敏感数据，符合长期审计需求。

立即采取行动

- **询问客户“您知道企业内有多少特权账号？都接触了哪些敏感数据？用什么方式在管理？”**
- **联系Security同事，安排POC**