

混合云时代, 完整的数据库安全平台

IBM Security Guardium 从源头保护数据, IBM Security Secret Server 特权账号鉴别和审计, 自动化应对 GDPR、CCPA、以及国内等保2.0 要求

随着国内《网络安全等级保护》(等保 2.0) 即将于 2019年 12月 01日实施, 国外欧盟《通用数据保护条例》(GDPR) 已于 2018年 5月 25日正式实施, 还有即将于 2020年 1月 1日生效的《加州消费者隐私法案》(CCPA), 如何应对国内外诸多法律规范的合规合法, 企业已经到了刻不容缓的时间点了。

在等保2.0 的安全计算环境中, 主要的测评重点包括了数据完整性和保密性的实现情况, 以及个人信息保护方面的技术机制和管理措施。另外在安全管理中心明确提出身份鉴别和审计的要求, 应对管理员 (包括系统管理员、审计管理员、安全管理员) 进行身份鉴别, 只允许其通过特定的命令或操作界面进行操作, 并对这些操作进行审计。也就是说, 数据安全平台和统一的特权账号管理和审计变成法规要求。

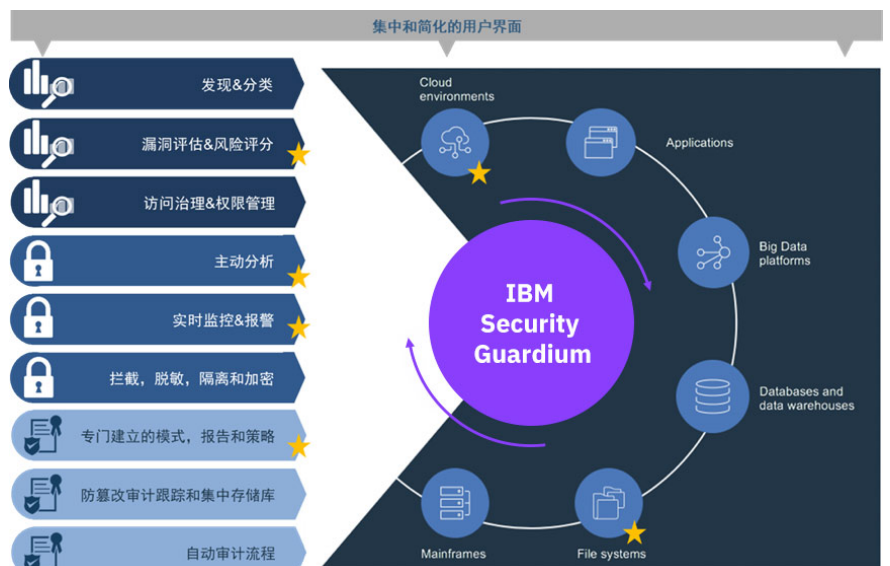
除了希望从源头来保护数据之外, 也需要从数据泄漏的管道来关注数据安全。在已知的安全泄漏中, 80% 与“特权账号密码”有关。因此自 2018年开始, Gartner 连续两年将“特权账号安全”在十大网络安全项目中排序第一。可见数据安全防护并不是一蹴而就的, 因此, IBM 针对数据安全防护平台, 推出了一套组合拳。

IBM Guardium 敏感数据保护

帮助您识别并防御各种内部威胁, 控制用户访问、监视敏感数据和分析活动。最大程度降低风险, 保护敏感数据免受威胁, 适应不断变化的环境。

IBM Security Secret Server 特权账号管理

管理和保护您企业中的特权账号, 并建立密码保险箱。



IBM Security Guardium 保护和审计功能优势所在

核心数据和敏感数据具有重要价值,易招致攻击。传统环境中,企业专注于边界防御系统的建设,但是随着更多的企业选择云环境部署数据库系统,传统的边界防御工具无法应对现有威胁的变化,包含源于社会工程学的组织内部攻击,使得数据库安全无法保障。

除了法规限定之外,云计算的趋势也不容忽视。越来越多的企业将业务搬迁至云上,然而,混合云场景下数据库管理存在很多挑战,比如:数据库种类、运行环境复杂、开发部署和运维难度大且易出错,稳定性难以得到保障等。目前正处于年末整理复盘之际,企业在制定明年 IT 预算时有必要考虑混合云趋势下的数据库安全平台项目。

数据库安全平台 Guardium 使用运行在操作系统层的轻量级探针,仅是对数据库操作流量数据的转发,不在数据库服务器上进行处理,与数据库管理系统无关,所以不影响正常的数据库操作。Guardium 可以完整地采集数据库操作活动数据,无论是基于网络访问、本地访问还是加密,这意味着无论是谁、何时何地访问了哪些数据资源都会被监控并记录。与此同时,在云环境下部署,也因为其运行在操作系统层而不受影响。无论是虚拟机还是物理机,只要运行的操作系统不变,Guardium 就可以正常工作。同时,针对于运行在容器中的数据库,也可以通过外部探针的方式捕获流量数据。

“自动化合规”也是大多数数据库审计工具用户的主要需求。Guardium GDPR Accelerator 能帮助用户高效评估与 GDPR 相关个人数据有关的安全与合规风险。因为组织合规本身是一个成本很高的过程,在实际过程中还需完成很多额外的工作。而 Guardium 本身内嵌了大量的用于合规的最佳实践。例如:金融行业的 PCI DSS (第三方支付行业数据安全标准)、SOX (萨班斯法案)、SAS70、ISO 27001/2 以及“数据隐私法”等甚至还没在中国大陆正式推行的相关规定,都包含在 Guardium 其中。这无疑给用户的合规带来了极大的便利。

IBM Security Secret Server 主要使用场景:



IBM Security Secret Server 管理和审计功能优势所在:

特权账号对于最敏感数据有存取权限,所以必须控制哪些人能够拥有这些特权并加以管理,同时在他们执行操作时进行监控。从特权账号管理(PAM)来看,最危险的安全威胁不只是来自于外部,而是来自于内部人员可以接触最宝贵的数据。所以必须对“皇冠上的明珠”的保护坚守最后一道防线。

IBM Security Secret Server 能自动发现特权账号并进行纳管,可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。Secret Server + Guardium data protection 根据企业详细信息(每个数据访问项:谁、什么、在哪、何时、为何)实时监控所有数据访问操作,以检测未授权的操作,帮助防止享有特权的内部人员和潜在的黑客进行未经授权的可疑活动,使得复杂的企业数据安全控制自动化、智能化。

特权账号管理更大的挑战,不仅是在于传统认知的系统管理员等人类特权账号管理,更难的在于应用系统中中和配置文件中的特权账号,这些特权账号无法透过管理手段解决,必须透过工具有效管理。IBM Security Secret Server 能有效的发现和管理应用系统和配置文件中的特权账号,并可以结合特殊情况下特权账号审批流程,来达到更高层次更全面的特权账号管理。

- **监控及控制:** 准确了解用户特权帐户的使用时间、方式和原因, 通过限制权限来提高端点安全性, 停止端点上的恶意软件。

- **安全及保护:** 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。

IBM 整体优势

波耐蒙研究所(Ponemon institute)对 183名目前使用 Guardium 的美国 IT 和 IT 安全从业人员进行调查研究, 结果显示 Guardium 显著提高了检测威胁能力。数据还显示该系统显著提高了跨复杂 IT 环境和企业管理数据风险的能力; 在识别和纠正数据安全问题上花费更少的时间; 漏洞和错位配置率显著降低, 有助于数据的准确分类; 遵从于 GDPR 等法规, 降低组织合规花费时间。

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。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。而这些安全平台可以和 IBM 其他安全产品无缝整合, 构建一个整体安全防护网, 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。

市场优惠促销套装 (研拟中)



优惠价#1: IBM Security Guardium, 5个数据源, 特价 30万元。

产品号	产品名	建议售价(RMB)	数量
D1NE3LL	IBM SECURITY GUARDIUM DATA PROTECTION FOR DATABASES RESOURCE VALUE UNIT (MVS) LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	306,534.20	5
D0THSLL	IBM SECURITY GUARDIUM COLLECTOR SOFTWARE APPLIANCE INSTALL LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	14,267.26	1

* limited time offer to Dec. 31, 2019.



优惠价#2: 5个 IBM Security Secret Server for Privileged Users, 特价 5万元。

产品号	产品名	建议售价(RMB)	数量
D21ZQLL	IBM SECURITY SECRET SERVER FOR PRIVILEGED USERS PER USER VALUE UNIT LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	47,675.25	5
D0THSLL	IBM SECURITY GUARDIUM COLLECTOR SOFTWARE APPLIANCE INSTALL LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	14,267.26	1

* limited time offer to Dec. 31, 2019.

即刻访问 IBM 安全官方网站

https://www.ibm.com/cn-zh/security?lnk=mpr_buse_cnzh&lnk2=learnquick



扫一扫，
关注 IBM 安全微信，
获取应对企业安全问题的
全球资讯

致电垂询 IBM 安全专家
400 810 1818 转 2395
(工作日 9:00 – 17:00)



IBM、IBM 徽标和 ibm.com 是 International Business Machines Corp. 在全球许多司法管辖区域的注册商标。其他产品和服务名称可能为 IBM 或其他公司的注册商标。Web 站点 www.ibm.com/legal/copytrade.shtml 上的“Copyright and trademark information”部分中包含了 IBM 商标的最新列表。

本文档为自最初公布日期起的最新版本，IBM 可能会随时对其进行更改。IBM 并不一定在开展业务的所有国家或地区提供所有这些产品或服务。

客户应遵守适用的法律法规。IBM 不提供法律建议或表述或保证其服务或产品会确保客户符合法律法规的规定。

本文档内的信息“按现状”提供，不附有任何种类（无论是明示的还是默示的）保证，包括不附有关于适销性、适用于某种特定用途的任何保证以及非侵权的任何保证或条件。IBM 产品根据其提供时所依据协议的条款和条件获得保证。



请回收使用