保护您的业务数据安全

IBM Security Guardium 有助于分析、保护和调整综合数据保护

亮点

- 采用主动、整体的方法来保护各个平台上的关键数据，包括主要数据库、数据仓库、大数据平台、云环境和文件系统等
- 降低总体拥有成本，自动发现敏感数据，发现风险并采取行动
- 利用加密、隐藏、修订、活动监控、动态拦截、提示和隔离，保护敏感数据免于遭受威胁
- 利用数据合规自动化在正确的时间将正确的报告发送给正确的人员
- 适应 IT 状况并支持全数据保护旅程

当今，数据安全漏洞越来越普遍，其影响也越来越大。全球研究表明，数据泄露的平均总成本现在高达 400 万美元。[1] 此外，商业机密、产品设计或其他知识产权方面的损失也会给企业带来经济损失。由于关键数据和敏感数据具有重要价值，因此它不仅仅是业务互动的核心，而且还是一种极具吸引力的攻击目标。

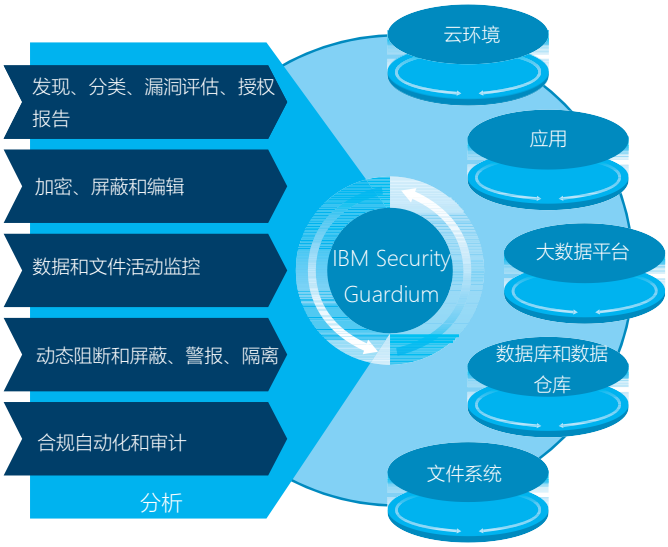
在以往，企业一直专注于可保护其关键信息的"周边"防御系统。但杀毒软件和防火墙等传统工具并不能解决当今的高级威胁问题，而在多数情况下，这些威胁都来自于组织内部。此外，数据一直在扩展、变化和移动，因此数据保护措施必须能够适应数据的具体状况。越来越多的用户、应用和系统需要即时访问不同的敏感数据 - 这些数据以直接存储或副本的形式存在于数据库、数据仓库、文件共享、大数据平台、云环境及其他环境中。对访问这种动态、分布式且不同的数据的人员以及共享数据的人员进行持续跟踪看起来似乎是一个不可能完成的任务。

IBM® Security Guardium® 旨在保护任何位置的关键数据。借助这种综合的数据保护平台，安全团队可自动分析数据环境中发生的状况，从而防范风险，帮助敏感数据抵御内外部威胁，同时无缝地适应影响数据安全与合规性的更改。

依靠综合数据安全

依靠综合数据安全，Guardium 可提供一种综合的方法来保护企业的"宝贵信息"- 对于业务成功和生存至关重要的关键信息。借助该解决方案的端到端图形用户界面，无论对于静态数据还是动态数据，安全团队均可识别和修复敏感数据的风险。而且这种统一的方法可扩展至各种结构化数据存储库和非结构化数据存储库中，包括数据库、数据仓库、 Hadoop、NoSQL、内存系统和文件共享。

实际上，Guardium 能够以一种可扩展、具有成本效益的方法灵活满足各种数据安全和保护要求 - 从基本合规性到综合数据保护。这种多层解决方案包括自动化数据威胁分析、动态数据保护和企业级可见性，进而可适应敏感数据环境中的变化。



Guardium 可在当今的异构环境中利用认知分析和自动化帮助保护关键数据。

分析敏感数据威胁

为了实现有效的数据保护，企业需要了解如何才能全面地保护数据。Guardium 有助于安全团队实现以下目标：

- 自动发现、分类敏感数据与权限并发现合规风险
- 了解谁在访问数据、观察异常并防止数据损失
- 迅速分析数据使用模式，以便发现并修复风险
- 通过自动化的高级分析和机器学习找出并制止异常的高风险行为，为分析流程提供支持
- 利用专业化的威胁检测分析尽早找出和制止数据泄露，比如找出并预警 SQL 注入或恶意的存储过程
- 提供相应的仪表板，帮助关键利益相关者随着时间的推移查看数据安全和/或合规状态及进展，以便更好地了解该计划如何实现业务增值，同时了解差距

Guardium 可帮助安全团队从易于使用的图形用户界面范围内自动发现并分类敏感信息。安全人员可利用系列步骤发现包含敏感信息的所有数据源（包括非编目数据库），之后可利用定制分类标签和授权管理功能自动执行安全策略。敏感数据发现还可用于定期阻止欺诈服务器并确保不会丢失关键信息。

为了执行策略并保护敏感数据，Guardium 可持续对访问（或试图访问）敏感数据的人员进行实时监控。除传统数据监控外，Guardium 还具备异常值检测功能，同时其基于行为变化进行分析及风险了解方面的智能也得到了提升。该解决方案使用高级机器学习算法，基于详细的情境信息（即每次数据访问的"对象、主题、地点、时间及方式"）监测异常数据访问。借助一种适应性学习流程，它可在积累时将正常活动模式与新的活动进行比较。其直观的认知型用户界面有助于指出异常状况，这样管理员就可深入研究其根本原因。

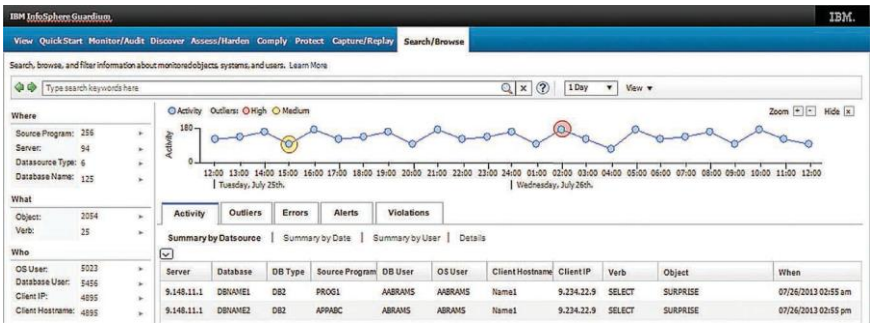
除“向下钻取”功能外，Guardium 还有助于安全人员在界面内迅速搜索审计报告和其它项目，同时对数据自身进行迅速的企业级搜索。不需要了解底层拓扑结构、聚合或负载平衡计划。搜索请求有助于从特定数据访问活动中提取洞察力，并可关注于特定的数据源、用户或日期。新的调查仪表板也有助于显示数据中的各种模式、异常和关系，进而有助于利用最佳实践默认视图来缩小范围。还存在一种连接配置工具，该工具可报告对于特定数据源的所有尝试连接。

保护敏感数据

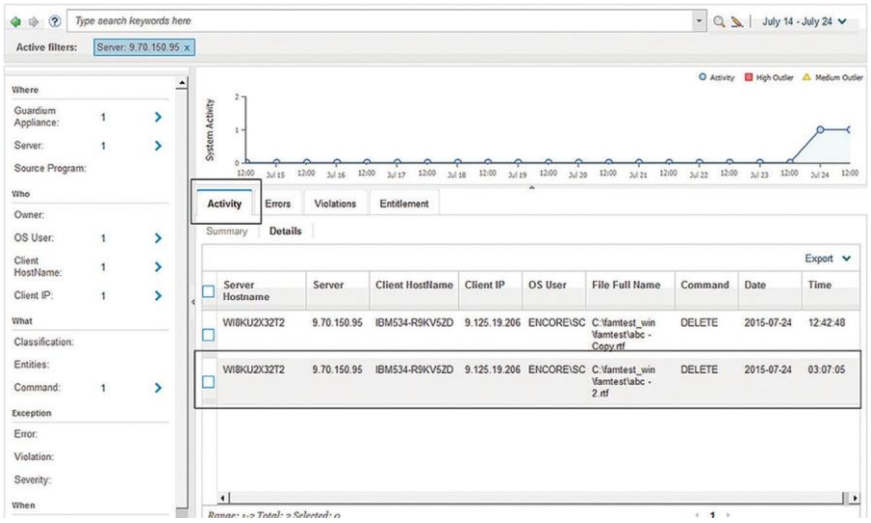
不断升级的敏感数据威胁和越来越多的合规性要求使得企业不得不重新思考其数据保护战略。Guardium 有助于安全团队实现以下目标：

- 借助自动化数据合规性和广泛的审计功能保护企业免于遭受财务风险
- 利用加密、隐藏、修订、动态拦截、报警和隔离，控制关键数据
- 利用实时活动监控和拦截，阻断内部或外部对于数据和文件的非法访问

Guardium 有助于利用安全、防篡改的审核轨迹来捕捉并审查所有敏感数据流量，包括特权用户的本地访问情况。实际上，它可为企业级合规报告、性能优化、调查和取证提供一种单一、集中且规范化的审计库。借助符合 Sarbanes-Oxley (SOX)、支付卡行业数据安全标准 (PCI DSS) 和数据隐私法规的预配置报告，企业可实现整个数据合规流程（包括报告分布、监督团队、签署和升级）的自动化。



Guardium 可提供一种方便的图形界面，可识别并响应智能算法检测出的异常值。



借助文件活动监控，Guardium 有助于企业监测并拦截文档数据相关的可疑活动（即使是特权用户的可疑活动）。

此外，Guardium 还可帮助安全团队利用基于文件的加密、数据库与大数据漏洞评估、静态数据隐藏和修订功能保护敏感数据免于遭受内外部威胁。它还可支持动态、实时数据隐藏和加密，并对可疑用户进行拦截、提示和隔离。事实上，它可限制非法人员访问大部分来源的敏感数据，包括云环境、大数据平台和文件系统。

Guardium 还有助于进行职责划分并持续监控所有敏感数据活动，包括实时监控文件系统访问情况。它有助于企业监测、记录并拦截特权用户的非授权活动和可疑活动。举例来说，Guardium 可检测各种敏感文件或目录，监测特定管理员的文件访问活动的飙升现象，生成对于不当访问的提示，拦截对于最敏感文件的访问并生成所有活动的自定义报告。Guardium 还有助于发现数据库和大数据基础架构中的漏洞，确保强化数据基础。

适应变化

数据基础架构在不断变化和发展，这使得应对新的、不断变化的安全问题成为一种挑战且需要付出高昂成本。Guardium 有助于企业：

- 支持传统数据技术和颠覆性数据技术，如 Hadoop、NoSQL 和云
- 轻松扩展数据保护架构，从监管合规性扩展至综合数据保护
- 在整个数据环境中利用单一数据保护基础架构（可实现自动负载平衡的一种基础架构）降低成本并改进结果

Guardium 有助于企业适应数据环境的变化，进而将数据保护扩展至应对新的用户、平台和数据类型。它还提供了一个平台，而该平台能够通过自动化、集中化和集成将 IT 运营方式融为一体，进而简化数据安全的管理流程。此外，国防信息系统管理局 (DISA) 颁发的运营许可证 (ATO) 等开箱即用型证书，或《一般数据保护法案 (GDPR)》等关键法规的合规性加速器也包含在其中，以方便最终用户使用。这一广泛的平台可支持传统数据库、云环境、基于 Hadoop 的系统、NoSQL、内存中系统和文件系统。Guardium 可提供灵活的可控性，以便于您针对特定的合规要求进行部署，同时进行轻松扩展，确保可随着业务需求的演变而提供额外保护。

与局部解决方案不同，Guardium 可支持与其它行业领先的安全解决方案、漏洞标准、应用等进行异构集成。Guardium 还可与 IBM QRadar® SIEM 等 IBM Security 解决方案进行最佳集成，从而可进行主动数据保护。Guardium 可将其事件和数据库发现/分类信息发送至 QRadar SIEM，进而可更有效地关联威胁活动。此外，Guardium 还可收到 QRadar SIEM 的状态和提示通知，进而可防范非法 IP 源、非法用户和新的漏洞，无论这些非法 IP 源、非法用户和新的漏洞位于应用、操作系统还是其它数据源中。举例来说，Guardium 和 QRadar 进行集成有助于企业通过应用避免潜在攻击、检测数据库攻击（如通过 SQL 注入）、在提取数据之前对其进行拦截并识别应用层的漏洞，从而实现虚拟修复补救。

Guardium 可在诸多行业实现价值

- 某家大型保险公司现在仅需一位全职员工即可管理约 1,000 个数据库的安全问题。
- 某家公用设施公司不到一年就实现了 55% 的投资回报，进而可确保 450 万客户遵守 SOX 和 PCI。
- 某家全球性银行可实时监控 5,000 多个数据源（包括大数据交易），同时不影响关键应用的性能。
- 某家国际电信公司现在可在分布于全球 16 个数据中心的数千数据库上实时集中监控并响应数据访问活动。
- 某家汽车制造商可监控和审核 500 个生产数据库，进而可提高安全性，同时将其安全员工的要求减少 90%。

为什么选择 IBM?

IBM Security 解决方案是全球企业进行高级数据保护的信赖之选。这些经验证的技术有助于企业保护其最关键的资源免于遭受最新的安全威胁。随着新的威胁的出现，IBM 可帮助企业通过各种产品、服务和业务合作伙伴解决方案构建其核心安全基础架构。

IBM 具有一些高度监管行业（包括治理、医疗卫生和金融服务）的全球服务交付专业知识。作为策略合作伙伴，IBM 帮助组织在极度复杂的 IT 环境中减少安全漏洞，管理风险。

有关更多信息

如欲了解有关 IBM Security Guardium 的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：ibm.com/guardium

关于 IBM Security 解决方案

IBM Security 可以提供最先进、集成的企业安全产品和服务组合。世界知名的 IBM X-Force® 研发支持的这一组合可提供安全情报，帮助企业全面保护其人员、基础架构、数据和应用，进而提供能够识别并访问管理、数据库安全、应用开发、风险管理、终端管理、网络安全等的解决方案。这些解决方案可以帮助企业有效管理风险，为移动、云、社交媒体和其他企业业务架构落实集成安全。IBM 作为世界上覆盖范围最广的安全研究、开发和交付企业之一，每天对 130 多个国家/地区的 130 亿个安全事件进行监控，并拥有 3,000 多项安全专利。

IBM Security
New Orchard Road
Armonk, NY 10504

美国印刷
2017 年 6 月

1 《2016 年数据漏洞成本研究：Global Analysis”. *Ponemon Institute*. 2016 年 6 月. ibm.com/security/data-breach/