提升您的“游戏”：

让数据安全更上一层楼

通过安全特定的大数据湖助力确保安全性与合规性的五大优势

在过去的 150 年里，全球的很多财富都来自于海量石油储量的发现与开采。不过，我们现在已经进入了一个转型的时代。《经济学人》近期的一篇文章指出：“全球最宝贵的资源已经不再是石油，而是数据。”[1]

无论这两者的相对价值如何，这两种商品之间的对比其实非常明显。全球石油储量是有限的，但数据积累的潜力是无限的。此外，数据“储备”时刻都在呈指数级增长。据 IDC 预测，到 2025 年，全球累积的数据量将有望达到 163 ZB。在这些数据中，几乎 20% 的数据“对我们的生活至为关键”，10% 的数据将会变得“异常关键”。[2]

石油必须经过采集并提炼后才能发挥其经济价值。对于数据而言，同样如此。正如来自全球经济论坛的 Adam Schlosser 在《财经内幕》上发表的一篇文章中所说：“数据也需要收集和维护，使其始终保持为可使用且可访问的格式，这样才能实现其经济价值。”不过，许多组织在管理数据这一宝贵财富方面做得非常不到位。Schlosser 写道：“就目前而言，在所有的数据中，仅有 10% 的数据在收集后的格式方面满足可轻松分析与共享的要求。”如此一来，组织就面临着会浪费其数据中潜藏的潜在财富的风险；如果仅仅是简单地收集数据，而不制定有效的战略，就会带来不可预测的风险、成本和运营挑战。[3]

随着时间的推移，组织将会收集并存储更多的数据，随之将会出现一系列问题和挑战：

- 如何优化数据安全架构和收集流程？
- 如何减少运营投入与成本，同时更快速的获取洞察力？
- 如何在合规性要求越来越多、时间越来越紧迫的情况下应对前述挑战？

尽管组织可以通过在更长的时间内保留更多的数据来改善其审计和分析结果，但这种做法本身也会增加风险和成本，并对性能带来更多的影响。在此情况下，组织如何才能在解决这些挑战的同时从数据中发掘更深入的洞察力？

本文将为您介绍组织在进一步提升数据安全与合规性并妥善安排多个优先事项的过程中可能会面临的障碍，这些障碍包括：

- 海量数据管理带来的管理需求
- 在更长的时间内保留海量数据的需求
- 维持或改善报告性能/速度的需求
- 为许多不同角色、职责的用户提供直接数据访问服务（即“释放”数据）的需求
- 在为审计数据补充其他类型的相关安全与合规性数据的同时也对这些数据执行复杂分析来发现新风险和/或洞察力的需求

接下来，本文将深入探讨组织如何采取有效的措施解决前述障碍，并通过这些措施将数据安全与合规性管理的效率和成效提升到一个新的高度。

敏感数据难题

数据管理员、IT 团队和信息安全专业人员一直都在努力跟上敏感数据的步伐。所有的敏感数据必须予以保护，但是查找、收集、管理并存储这些数据本身也是一个巨大挑战。“压迫”系统或环境的数据量越多，生成分析所需的时间就越长。因此，往往需要耗费数小时，甚至有些情况下要耗费数天，才能生成报告。如果负责提供数据输入的数据来源在安全级别上不稳定，就会导致安全一直处于风险之中。

我们必须在整个技术格局中进行数据安全与合规性投入，不过这种格局也是不断变化的：数据量会不断扩展、工作负载不断变化、合规性需求在不断增多，而且确保支持所需的处理能力也越来越高。

相应地，随着时间的推移，组织会收集并存储越来越多的安全数据，因此需要解决以下问题：

- 您如何应对《医疗保险可携性和责任法案 (HIPAA)》或 Sarbanes-Oxley (SOX) 等合规性法规中的长期数据存储要求带来的挑战？
- 您（或您的数据库管理员）如何向审计人员等关键利益相关者快速交付数据报告？
- 您的基础架构是否具有海量数据存储所需的容量和处理能力？您目前采取哪些措施来解决系统性能问题？
- 随着数据存储要求的不断增多，您如何解决不断攀升的存储成本？
- 您目前采用何种方法来整合情境感知的数据并通过分析获得可执行的洞察力？
- 您如何访问并关联来自大量各种来源（比如开票技术、人力资源或客户关系管理应用，以及 QRadar SIEM、Splunk、CyberArk、ServiceNowdeng 等应用）且需要加以利用的数据？
- 您目前采用哪些措施针对任何给定的数据库或其他数据来源构建全方位的统一数据安全视图？
- 您如何在解决这些挑战的同时从数据中发掘更深入的洞察力？

安全特定的大数据湖如何让问题变得更简单？

在寻找上述问题的答案时，安全特定的大数据湖可为您提供帮助。该款技术解决方案提供了一个中央数据存储库，能够满足海量数据带来的需求，这些数据不仅包括审计数据及审计相关数据，还包括来自现有活动监控解决方案的安全数据，以及来自 HR 应用、大数据分析平台、SIEM 解决方案及 IAM 解决方案等其他来源的扩充数据。这将为数据安全、保护及审计计划提供支持。

该款解决方案支持以更快、更广泛的自助式方式访问各种报告和活动数据，因此可帮助数据库管理员卸去许多日常运营负担，使其无需再处理特定的临时请求。

在进行解决方案评估时，您应寻找那些可帮助您在以下领域实现改善的安全特定大数据平台：

- **敏捷性：**优化您的数据安全部署，简化数据收集和管理流程，减轻运营负担，改善性能，降低存储成本，并让用户能够随时随地直接访问他们所需的数据。
- **保留：**存储更多的审计数据和扩充数据，在不损及性能的情况下，满足更长的合规要求并构建情境感知的历史洞察力。
- **洞察力：**运用大数据分析和机器学习功能交付新的合规与数据安全洞察力，从扩展的数据集中发现新的风险领域及新的威胁范例。

IBM Security Guardium Big Data Intelligence 简介

从本质上来说，IBM Security Guardium Big Data Intelligence 是专为确保数据安全而构建的大数据湖。

Guardium Big Data Intelligence 能够汇聚、存储和分析数据，也能针对数据库、文件系统和大数据平台安全与合规、数据和文件活动监控、数据丢失防范 (DLP) 及其他来源提供报告和新洞察力。长期的高度精细化活动、漏洞、授权及审计信息可以合并到低成本的数据安全数据湖中，进而改善信息的访问水平，并帮助简化数据收集和管理流程，同时降低成本。

除了作为数据湖而提供的功能之外，Guardium Big Data Intelligence 还可提供许多其他独特的功能，包括对数据和风险洞察力的直接实时访问、灵活的事件级工作流管理及数据扩充功能。借助这些功能及其他功能，用户可以充分利用数据湖的丰富功能来改善安全性和审计结果，具体来说，可为您提供以下功能：

- **实时数据和风险洞察力：**该解决方案可为授权用户（如审计人员和安全分析师）提供安全、直接的访问功能和自助式报告功能，进而缩短获取洞察力所需的时间。如此一来，Guardium 管理员便可减少在数据管理与访问方面的投入，更多地专注于数据安全、数据保护和合规进展。

- **数据扩充：**使用低成本的存储在动态的大数据湖中存储数据安全及合规性信息，确保可通过来自其他业务流程和应用（如开票技术、人力资源或客户关系管理应用等）的相关数据、以成本高效的方式来扩充数据。借助经扩充的安全与合规数据，您便可进行更具情境感知性的分析，进而发掘新的洞察力。
- **灵活的工作流管理：**该解决方案使用自动化功能来高效、准确地协调数据安全及合规相关的任务。这种事件级的工作流工具可帮助有着不同需求的最终用户专注于与其相关的结果，无需审核和手动整理整个报告。该产品能够将报告中的每个条目分配到有关利益相关者的“虚拟队列”并通过可定制的工作流推动事件的进展。此外，角色和流程也可以定制化。
- **控制、策略与合规性：**借助该解决方案，审计人员和信息安全专业人员等用户可以根据需求控制和访问特定数据及数据洞察力。

Guardium Big Data Intelligence 还支持将确保合规性所需的数据至少保留 5 年的时间，也支持合规审计（SOX、HIPAA、GDPR、PCI 等）。所有的必需数据均存储在数据湖中。

Guardium Big Data Intelligence 是 IBM 数据安全与保护解决方案套件的有效补充，尤其是支持与 Guardium 数据保护解决方案的高效集成。

IBM Security Guardium Big Data Intelligence 的五大优势

IBM Security Guardium Big Data Intelligence 具有五大关键优势，可帮助企业降低成本、减少合规投入并发掘组织数据中潜藏的宝贵洞察力。具体来说，这些优势包括：

1. **收集、管理并存储海量数据的同时降低运营成本。**随着数据量的不断增加，存储成本也在不断攀升。不过，可作为大数据湖使用的 Guardium Big Data Intelligence 专为确保数据安全而构建。它有助于降低基础架构与运营开销，进而直接降低成本。事实上，经过实践证明，Guardium Big Data Intelligence 能够将基础架构和产品成本降低 25% 以上、将存储需求降低 80% 以上（基于 IBM 客户的部署）。

2. **在不影响性能的情况下支持更长的数据保留时间。**在某种程度上的“完美风暴”场景中，由于许多合规性法规都在存储时间长度方面提出了更多的要求，导致数据量呈指数级扩展。将更多的数据存储更长的时间，要么会导致系统性能下降，要么会增加容量和处理能力成本，或者两者兼而有之。Guardium Big Data Intelligence 的 NoSQL 平台可确保安全地存储海量数据，同时确保数据的可轻松访问性。此外，这种架构还支持在不损及相关性能的情况下，长期存储海量数据。
3. **更快速地交付数据安全、合规性和运营报告。**Guardium Big Data Intelligence 可提供近乎实时的报告功能。借助该功能，用户可以充分利用数据为组织带来最大的成效，同时减少在报告生成方面一般所预期的成本和时间投入。经实践证明，无论是在实验室测试中还是在生产部署中，该大数据平台在任何位置运行报告的速度可达到传统架构的 10 到 100 倍。某个用户曾介绍说，对于一个包含有 160 亿条记录的报告，之前需要两天的时间才能生成，而借助 Guardium Big Data Intelligence，只需 5 秒即可生成。
4. **基于来自多个来源的历史数据和扩充的数据执行大数据分析。**Guardium 可提供扩展的存储功能，进而提升历史数据的存储深度，而作为大数据湖，它能够从额外的来源拉取数据，进而实现数据的扩充，这样便可实现高级分析，为合规及数据安全提供支持。如此一来，更具情境感知性的分析便可发掘之前潜藏的宝贵洞察力。
5. **为经授权的最终用户和应用提供自助式报告访问服务。**自助服务式功能能够让安全与合规利益相关者随时随地访问所需的数据。如此一来，管理员便可减少在日常数据管理细节方面的时间投入，而更多地专注于提升数据安全、确保长期合规性。

跟上海量数据扩展的步伐

大数据时代为组织带来了大量机遇，使其能够妥善地管理和保护他们的数据“财富”。不过，随着数据量的不断增加，以及数据保留要求的不断延长，也为组织的数据安全及合规环境带来了之前从未预见过的压力。在此情况下，组织可部署经优化的安全数据湖，帮助他们提升敏捷性，进而减少这方面的压力。

IBM Security Guardium Big Data Intelligence 能够简化您的现有数据安全解决方案，缩短获取洞察力所需的时间，并降低运营、数据安全及合规相关的成本。Guardium Big Data Intelligence 能够将大量的历史数据及近乎实时的数据保留并处理更长的时间，使得团队能够快速地获取新的、经扩充的数据安全与合规洞察力，同时降低成本、提供自助式数据探索，并交付综合性的报告功能。

了解有关如何尽最大可能简化现有数据安全解决方案、缩短获取分析洞察力所需时间并降低成本的更多信息。敬请访问 IBM Security Guardium Big Data Intelligence 网站。

[1] https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

[2] https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

[3] http://www.businessinsider.com/data-is-not-the-new-oil-adam-schlosser-of-the-world-economic-forum-2018-1