# IBM Security Guardium Analyzer

欧盟出台的《通用数据保护条例》(GDPR) 是一项影响深远的重要法规，它体现了数据隐私性变得越来越重要。GDPR 有可能会颠覆数据持有者/处理者与数据相关的个人（即，数据主体）之间的关系。从 2018 年 5 月 28 日起，全球各地的企业只要处理涉及欧盟数据主体的个人数据，他们就需要遵守 GDPR 法规，不论这些数据在何处保存或处理。违规企业需要支付巨额罚款，最高可达到 2000 万欧元或者 4% 的全球年收入，详细信息请参见 GDPR 法规。

GDPR 要求影响了企业内部的多个不同的业务领域，包括数据隐私官、首席信息安全官、数据风险官、合规经理、数据经理和 IT 经理等等，所有这些群体都在想方设法了解如何高效管理 GDPR 要求，同时帮助企业走向成功。

IBM® Security Guardium® Analyzer 是一款软件即服务产品，它通过以下方式帮助合规经理、数据经理和 IT 经理启动 GDPR 之旅：定位内部数据库和云数据库中的 GDPR 相关个人数据；对这些数据进行分类；识别漏洞；并帮助用户了解从何处入手将风险降至最低。

通过使用 Guardium Analyzer，风险分析*结果*将被传输至云端，您可以在云端查看这些结果，而敏感的个人数据不会移动，依然保存在企业内部。该服务托管在 IBM 数据中心内。

亮点

- *高效评估与 GDPR 相关个人数据有关的安全与合规风险*
- *在内部数据库和云数据库中寻找 GDPR 个人数据；扫描数据库漏洞*
- *利用下一代数据分类功能寻找 GDPR 特定的个人数据和敏感的个人数据模式*
- *利用按优先级排序的风险评分结果和风险缓解建议，开始消除风险*

## GDPR 合规性分析即服务

Guardium Analyzer 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。它利用下一代分类技术和漏洞扫描功能，识别最有可能通不过 GDPR 相关审查的数据库，然后将风险降至最低。它会优先处理包含需要更多关注的高危个人数据和敏感个人数据的内部数据库和云数据库。

用户可以设置定期扫描数据库：为每个数据库选择一个扫描窗口，在对企业最合适的时机运行评估，然后设置数据库扫描频率（如每周或每月扫描一次）。扫描之后，结果和风险数据将发送至云端，用户可以在概览仪表板中查看结果和风险数据。


*交互式 Guardium Analyzer 仪表板显示潜在的 GDPR 相关风险信息。用户点击一下，深入挖掘更多详细信息。*

## 寻找 GDPR 相关个人数据

借助 Guardium Analyzer，企业能利用下一代分类引擎和预置的以 GDPR 为导向的数据模式，高效寻找和归类个人数据和敏感的个人数据，最终找到 GDPR 个人数据。在归类数据时，该服务不只是搜索顶层数据，它还会分析内部数据库和云数据库表中的文本，寻找并归类 GDPR 相关个人数据，比如个人身份识别码和性别等。

## 发现风险

数据库中的漏洞会提高敞口和风险级别，尤其是数据库中包含受 GDPR 监管的数据时更是如此。Guardium Analyzer 利用漏洞扫描和评估功能，高效扫描多种数据库漏洞。然后，它能够识别需要关注的可能被利用的最迫切的漏洞问题，比如 CVE 或缺失的补丁。

它会利用专业的风险评分技术处理 GDPR 分类结果和漏洞扫描结果。该产品能帮助您识别每个数据库的相关风险级别，它提供详细信息解释数据库中哪个部分有风险以及为何有风险，并提供具体的风险缓解建议。

## 采取行动

风险评分信息为授权用户提供按优先级排序的风险列表，为用户提供相关信息，帮助他们了解可能需要采取哪些措施来消除漏洞风险，保护 GDPR 相关个人数据。

Guardium Analyzer 还包含一个进度仪表板。该仪表板根据云端和内部的数据库环境的反复扫描结果以及风险评分和按优先级排序的风险缓解建议，展示随着时间的推移，风险级别的发展趋势与消除这些风险的进展情况。

## IBM Security Guardium Analyzer 的重要功能

Guardium Analyzer v1.0 提供的重要功能包括：

**连接云数据库和内部数据库。**帮助客户连接数据库，发现个人数据以及与受 GDPR 监管的数据有关的漏洞。客户可以同时连接多个数据库。该解决方案利用加密技术保护数据，个人数据不会被上传到云端，这是连接和扫描流程的环节之一。

Guardium Analyzer 支持 Oracle、Db2 和 MS SQL Server 数据库，包括内部数据库和云数据库。

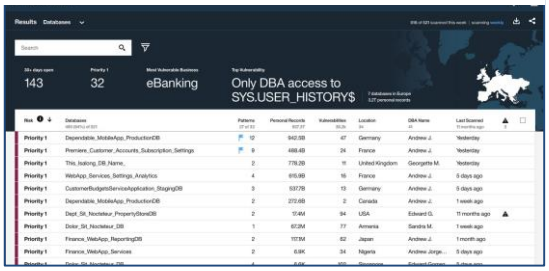
**下一代数据分类。**提供下一代分类引擎（它也支持 IBM Watson 产品）和以 GDPR 为导向的预置数据模式，帮助您高效识别和归类受 GDPR 监管的数据。分类引擎将扫描和分析内部数据库和云数据库中的文本，寻找并归类此类数据。用户可以利用 IBM 预置的 GDPR 数据模式、用户提供的数据模式，或者结合利用这两种数据模式。

**漏洞扫描。**数据库中的漏洞会提高敞口和风险级别。Guardium Analyzer 利用漏洞扫描和评估功能，高效扫描多种数据库漏洞。然后，它能够识别需要关注的可能被利用的最迫切的漏洞问题，比如 CVE。

**风险评分。**风险评分技术基于数据分类和漏洞扫描结果，交付按优先级排序的风险信息。风险评分是基于找到的个人数据量、找到的个人数据类型（敏感个人数据或者普通个人数据），以及找到的漏洞数量得出的。识别的风险数量最多的数据库被标记为优先级 1，风险数量最少的数据库被标记为优先级 3。该产品能帮助您识别每个数据库的相关风险级别，它提供详细信息解释数据库中哪个部分有风险以及为何有风险，帮助企业了解其数据库中有哪些类型的 GDPR 相关个人数据，以及企业的风险级别。

**按优先级排序的风险缓解建议。**

风险评分信息将用于向您和您的合规或安全团队展示按优先级排序的风险列表。




*从概览仪表板向下钻取，获取按优先级排序的详细信息，了解可能存在风险的数据库。*

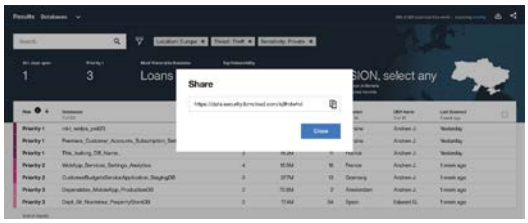
这些按优先级排序的风险将帮助用户了解他们应该采取哪些措施来消除漏洞风险，保护 GDPR 相关个人数据。这些建议将帮助企业按优先级排列关注点，降低 GDPR 相关风险。

用户可以按因素，比如风险严重性（优先级 1、2、3）、业务威胁、位置和数据模式，筛选列表。

## 简化 GDPR 相关活动

Guardium Analyzer 能帮助企业内不同类型的用户合作开展 GDPR 相关数据活动。该技术将帮助合规经理、数据经理和 IT 经理获取所需的信息和详细信息，推动他们围绕 GDPR 合规活动开展重点活动。

屏幕上将显示按优先级排列的风险详情和风险缓解建议，用户可以点击“共享”按钮，生成一个可发送给授权数据经理的链接。Guardium Analyzer 能够向每位数据经理发送他们所拥有的数据库的优先级列表。由此，数据经理可以登录或使用该链接，仅查看自己的数据库列表。这样，该解决方案就能支持职责分离。




*“共享”按钮将支持不同的团队和用户开展协作。*

数据库经理可以选择特定的数据库，查看找到的漏洞列表，然后点击获取漏洞详细信息，查看如何有效降低风险的建议。这样，数据库经理就能着手采取措施，降低 GDPR 相关风险和敞口。

## 为什么选择 IBM Security Guardium?

IBM Security Guardium Analyzer 平台为内部环境、云环境和混合环境提供全面的数据安全方法。这个广泛的 Guardium 数据安全和保护平台利用智能和自动化技术，提供集中的战略方法来保护各类敏感数据。强大的实时分析和适时分析功能可帮助安全团队分析风险格局，快速发现内外部威胁。该解决方案提供广泛的数据保护功能，其中包括：

- 针对各类敏感数据的自动化探索和归类
- 授权报告
- 漏洞评估与缓解
- 针对 NAS、SharePoint、Windows 和 Unix 存储库的数据和文件活动监控
- 屏蔽、加密、拦截、警报和隔离
- 自动化合规支持

Guardium 帮助安全团队保护当今异构环境、各个数据库、数据仓库、Hadoop、NoSQL、内存系统、文件和云环境中的敏感数据。该解决方案能够响应 IT 环境的变化，不论是增加新用户、扩展容量还是集成新技术。

## 有关更多信息

如欲了解有关本产品的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：https://www.ibm.com/cn-zh/marketplace/guardium-analyzer

## GDPR 免责声明

请注意：客户应负责确保其自身符合相关法律法规的要求，包括欧盟《通用数据保护条例》。在识别并解读可能会影响客户业务及客户依法采取的相应措施的任何相关法律法规要求时，客户应负责寻求合格律师的建议。本文档中所述的产品、服务及其他功能不一定适于所有客户的情况，可能会存在可用性受限的情况。IBM 并不提供法律、会计或审计建议，亦不承诺或保证其服务或产品可确保符合任何法律或法规。

点击此处，了解 IBM 自身在准备 GDPR 合规性方面的旅程及我们为确保您与 GDPR 的合规性而推出的相应功能和产品。

IBM Security
75 Binney St
Cambridge, MA 02142

美国印刷
2018 年 5 月