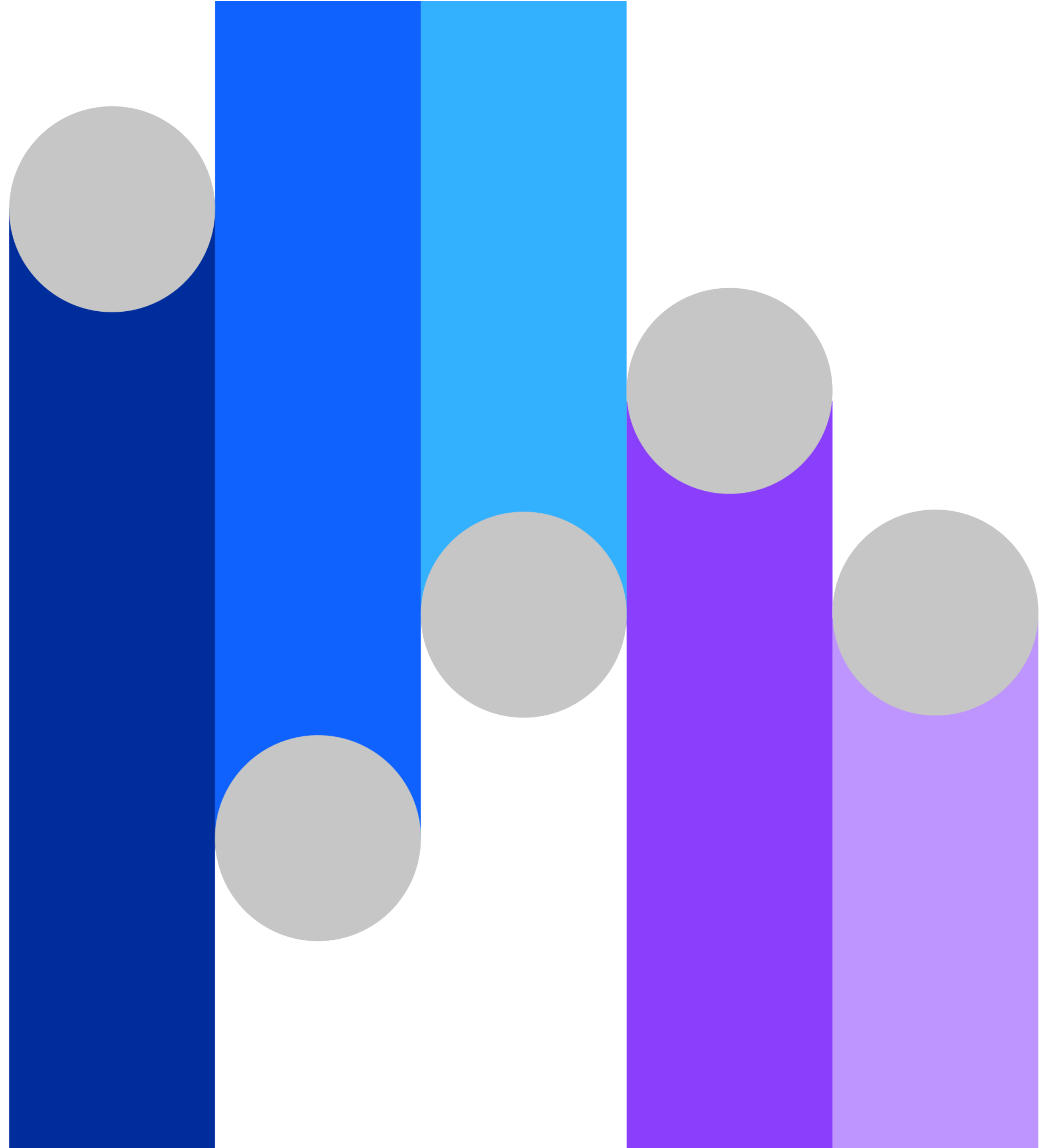


应避免的五种 常见数据安全 陷阱

了解如何提升数据安全性和合
规性状况



目录

[00 →](#)

简介

[01 →](#)

陷阱 1:

未能超越合规性

[02 →](#)

陷阱 2:

未能认识到集中式数据安全
的必要性

[03 →](#)

陷阱 3:

未能定义数据的负责人

[04 →](#)

陷阱 4:

未能解决已知漏洞

[05 →](#)

陷阱 5:

未能确定现代数据
活动监控的优先级
并对其加以利用

[06 →](#)

未来有哪些发展愿景?

[07 →](#)

为什么选择 IBM Security?

简介

数据安全应为企业的重中之重，而这背后有着充分的理由

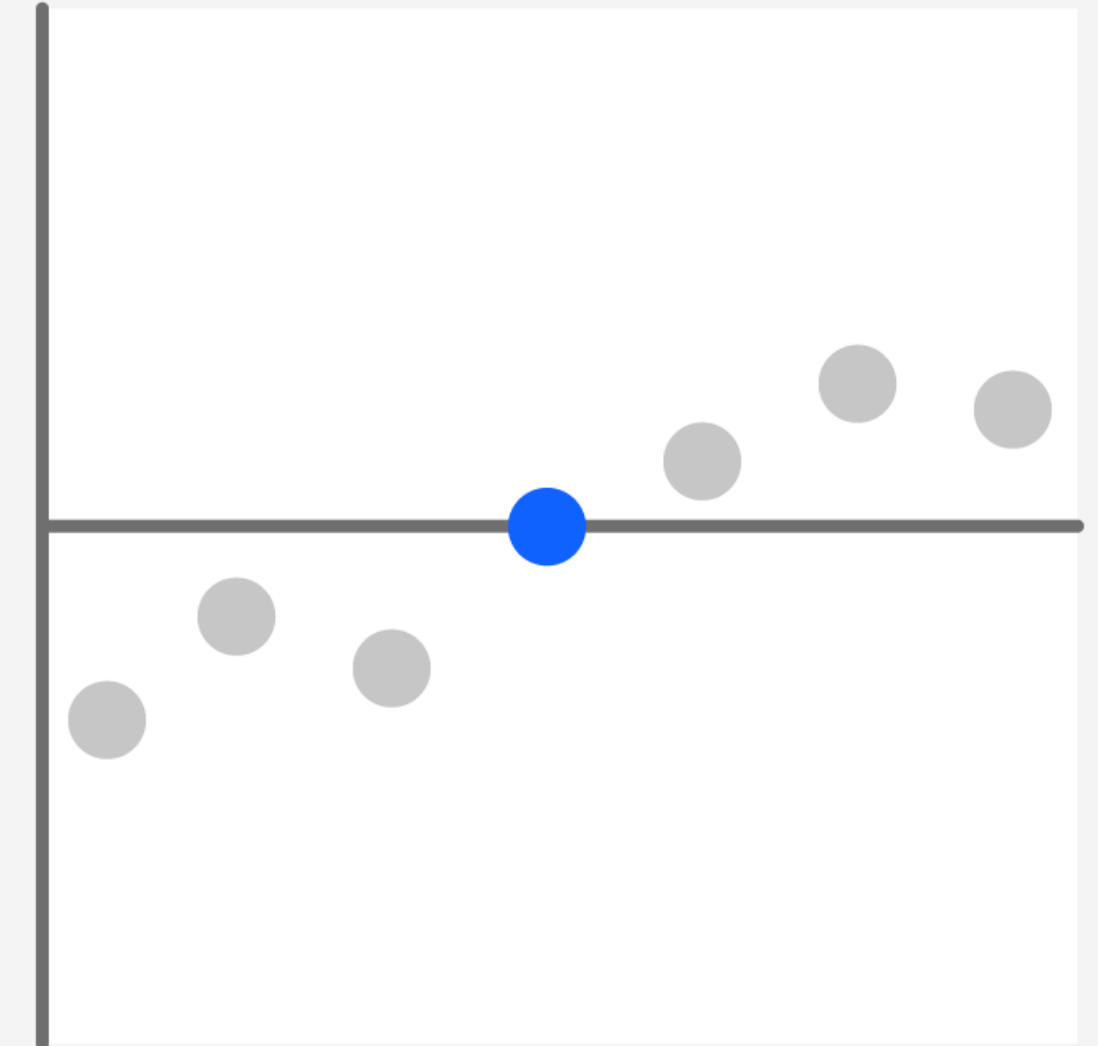
即使 IT 环境日趋分散和复杂，但有必要明白，很多数据泄露其实本可预防。虽然各个公司面临的网络安全挑战和目标可能有所不同，但组织在开始解决数据安全问题时却常犯同样的普遍错误。更为重要的是，很多企业领导层常将这些错误视为正常的商业惯例。

导致攻击者成功发起网络攻击的内外部因素包括如下几项：

- 网络边界的侵蚀
- 更复杂的 IT 环境会暴露更大的攻击面
- 云服务对网络安全实践的需求不断增长
- 网络犯罪的性质日趋复杂化
- 网络安全技能呈现持续短缺
- 员工缺乏对数据安全风险的感知

445 万美元

2023 年，全球数据泄露的平均成本出现上升，3 年内增长了 15%。¹



陷阱 1：未能超越合规性

合规性不一定等同于数据安全性。如果企业将有限的数据安全资源集中用于符合审计或认证要求, 就会变得固步自封。很多大规模数据泄露就发生于纸面上完全合规的组织当中。以下示例说明仅关注合规性会如何削弱有效安全性。

覆盖范围存在缺失

在接受年度审计之前, 企业常争先恐后地忙于处理地址数据库配置错误和过时的访问策略。漏洞监控和风险评估应是持续开展的两项活动。

追求最低工作量

对很多企业来说, 采用数据安全解决方案只是为了满足法律要求或业务合作伙伴的要求。这种“让我们实施最低标准并回归业务”的心态可能会与良好的网络安全实践背道而驰。实现有效的数据安全是一场马拉松, 而不是短跑。

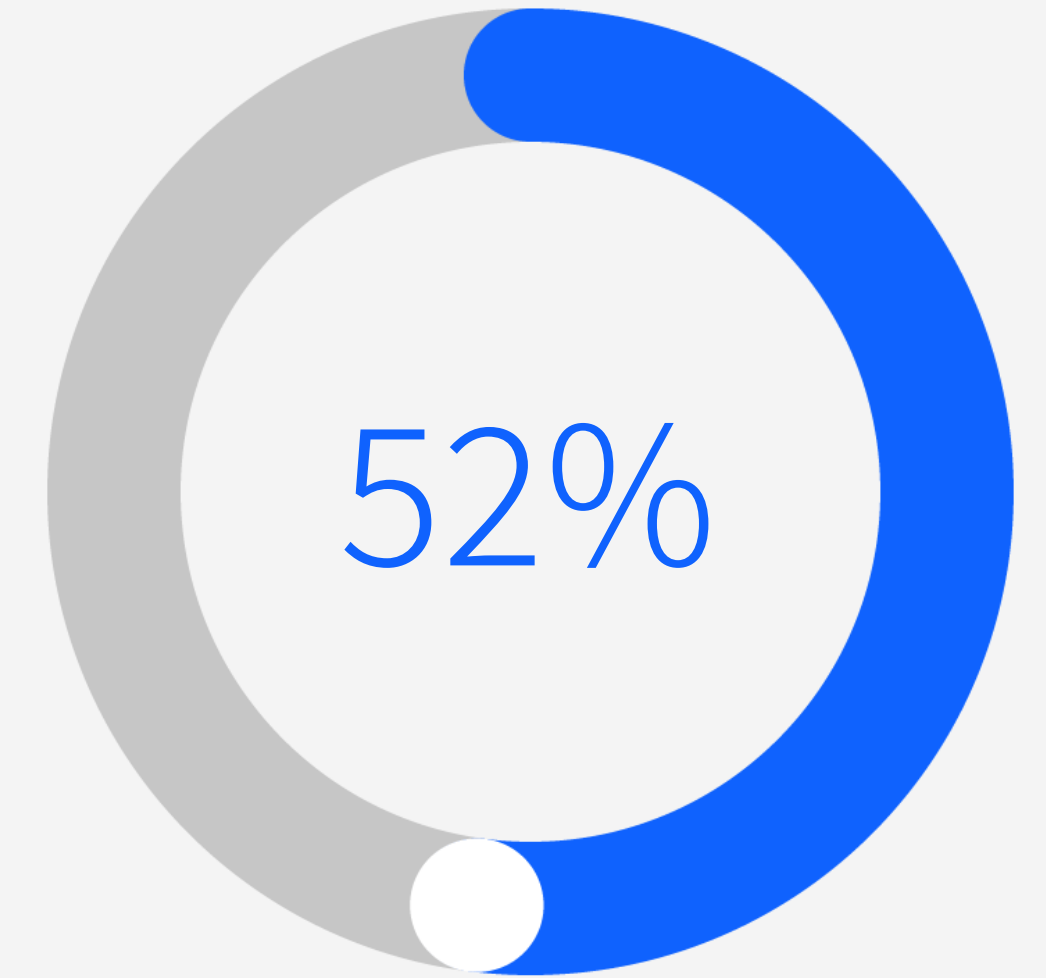
紧迫感逐渐消失

当法规相对成熟时, 企业可能会对控制措施的管理感到自满, 例如萨班斯法案 (SOX)、通用数据保护条例 (GDPR)、支付卡行业数据安全标准 (PCI DSS) 和加州隐私

权法案 (CPRA) (先前为 CCPA)。随着时间的推移, 领导层可能会减少对受管制数据在隐私、安全和保护方面的关注, 但与不合规相关的风险和成本却依然存在。

遗漏不受管制的数据

资产 (如知识产权) 一旦丢失或与未经授权的人员共享, 便可能会使您的组织面临风险。只关注合规性可能会导致数据安全组织忽视有价值的信息且对其保护不周。



52% 的组织表示, 将工作负载转移到公共云所带来的复杂性也增加了履行合规义务的难度。²

将合规视为创新和提高安全标准的机会, 以支持您的业务。

■ 解决方案: 认识并接受合规只是一个起点

数据安全组织必须制定战略计划, 从而始终如一地保护其业务的关键数据, 而不只是响应合规性要求。

数据安全和合规性计划应包括以下核心实践:

- 从本地、云数据存储和软件即服务 (SaaS) 应用程序中发现敏感数据, 并对其进行分类。
- 通过情境洞察和分析来评估风险。

- 通过加密和灵活的访问策略保护敏感数据。
- 监控数据访问和使用模式, 以快速发现可疑活动。
- 实时应对各种威胁。
- 简化合规及其报告。

最后一个要素可能包括与法规一致性相关的法律责任、企业可能遭受的损失以及不合规罚款之外其他损失产生的潜在成本。

最终, 您应全面审视要对其进行保护的数据的风险和价值。

陷阱 2: 未能认识到集中式数据安全的必要性

陷阱 2: 未能认识到 集中式数据安全的必要性

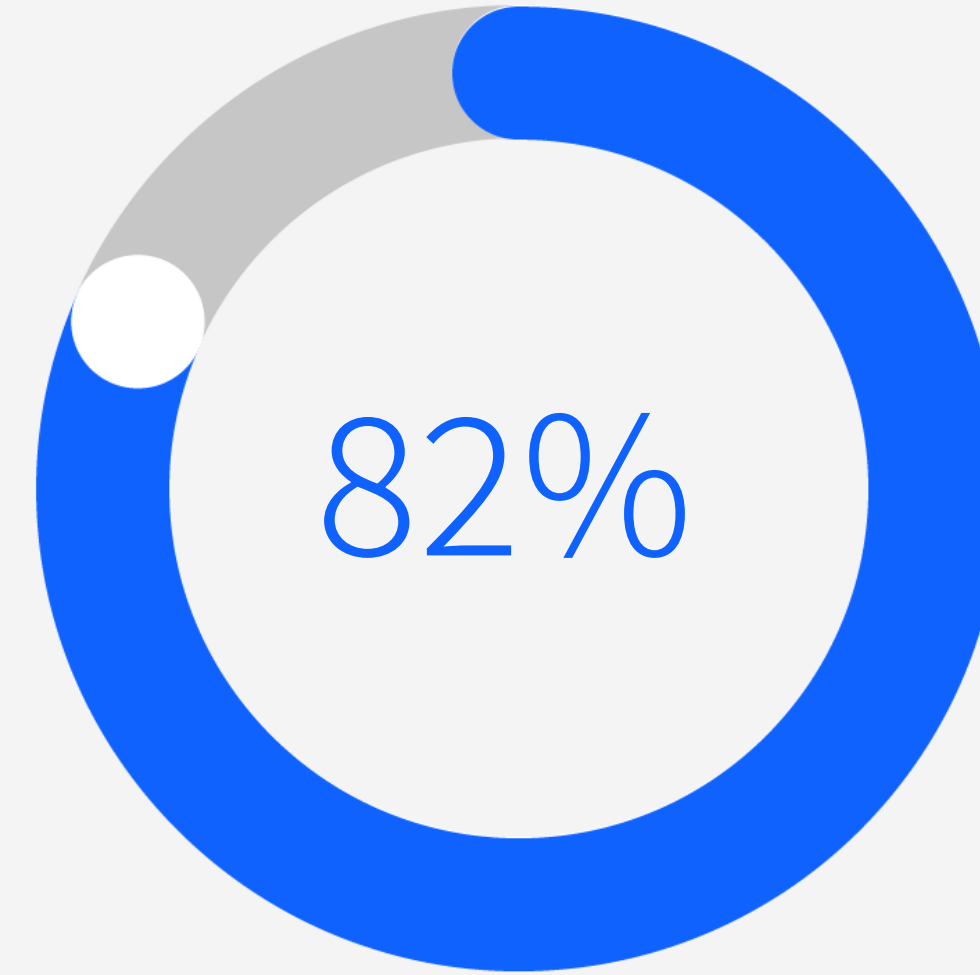
如果缺少涵盖数据隐私和安全性的更广泛合规要求, 组织领导层便可能会忽视对实现一致的企业级数据安全性的需求。

对于部署有不断变化和发展的混合多云环境的企业来说, 新型数据源可能每周或每天都会出现, 并极大地分散敏感数据。

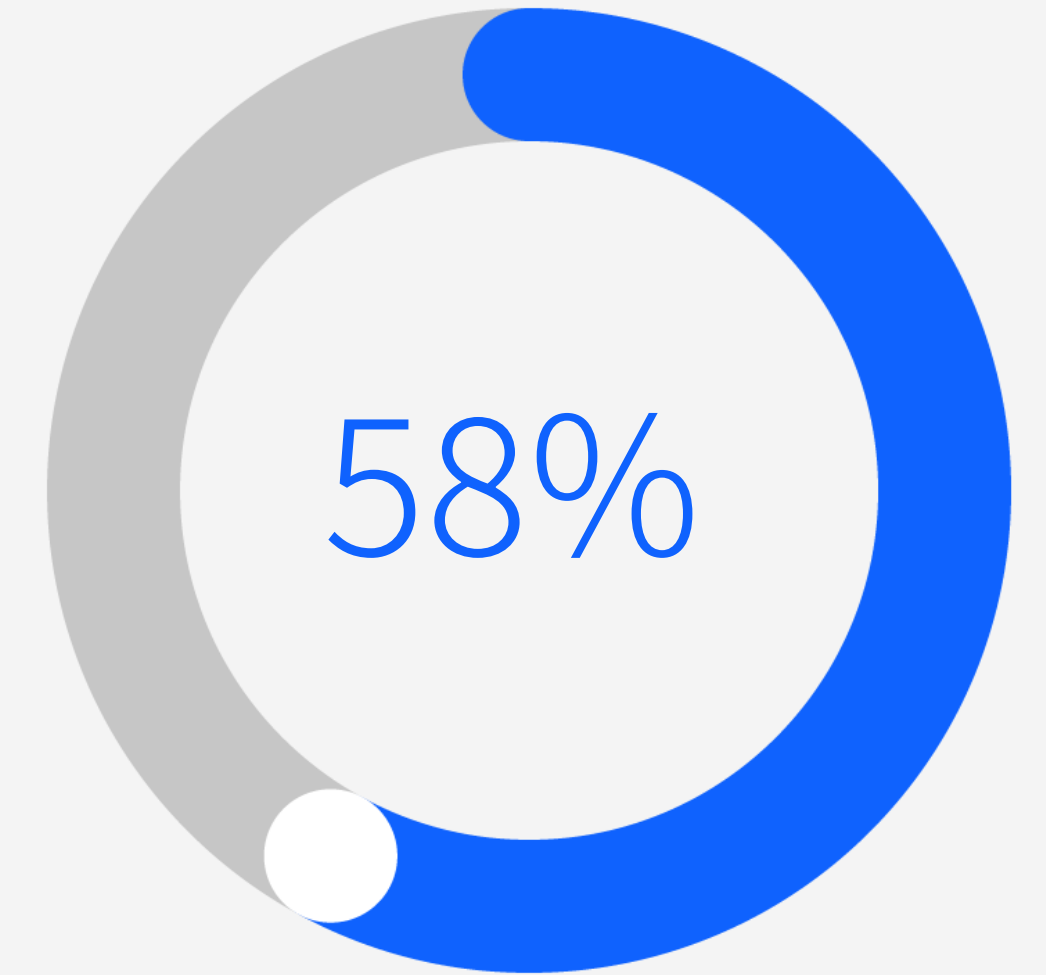
对于正在发展和扩展其 IT 基础架构的公司来说, 其领导层可能未意识到不断变化的攻击面所带来的风险。当其敏感数据在日益复杂且多样化的 IT 环境中移动时, 领导层可能缺乏足

够的相关可见性和控制力。如果不采用端到端数据隐私、安全和保护控制措施, 特别是在复杂的环境中, 就会造成代价高昂的疏忽。

在孤岛中运行网络安全解决方案可能会导致其他问题。例如, 部署有安全运营中心 (SOC) 和安全信息与事件管理 (SIEM) 解决方案的组织, 可能会疏于向这些系统提供从其数据安全解决方案中收集的洞察。同样, 安全团队、流程和工具之间缺乏互操作性可能会阻碍任意网络安全计划的成功落地。



82% 的泄露事件涉及存储在云端的数据。¹



58% 的组织表示, 它们有约 21% 到 50% 的云端敏感数据没有得到充分保护。²

保护敏感数据应与更广泛的网络安全工作相结合。

■ 解决方案:了解敏感数据的所在位置,包括本地、云托管存储库和 SaaS 应用程序

保护敏感数据应与更广泛的网络安全工作相结合。除了需要知道敏感数据的所在位置外,您还应了解何时以及如何访问这些数据,即使这些信息会瞬息万变。此外,您应努力将数据安全和保护洞察和策略与整体网络安全计划进行整合,从而实现不同技术之间的紧密协调通信。跨不同环境和平台运行的数据安全解决方案可在此过程中提供帮助。

何时才是将数据安全与其他网络安全控制措施整合为更全面的网络安全实践的合适时机?出现以下迹象时,表明您的组织可能已准备好采取此后续步骤。

丢失宝贵数据的风险

组织的个人、敏感和专有数据的价值巨大,其损失会对企业的生存能力造成严重损害。

陷阱 2: 未能认识到 集中式数据安全的必要性

监管影响

组织会根据法律要求收集和存储数据, 例如信用卡号、其他付款信息或个人数据。

缺乏网络安全监督

组织已发展到难以跟踪和保护所有网络端点(包括云实例)的程度。例如, 您是否清楚在本地、云数据存储和 SaaS 应用程序中存储、共享和访问的数据的相关操作位置、时间和方式?

评估不充分

组织采用了一种不成体系的方法, 通过其无法明确了解所有网络安全活动的确切支出。例如, 针对为降低数据安全风险而分配的资源, 您是否有适当的流程来准确度量投资回报率(ROI)?

如果您的组织遇到上述情况, 则应考虑获取必要的网络安全技能和解决方案, 以便将数据安全纳入更广泛的现有安全实践中。



陷阱3：未能定义 数据的负责人

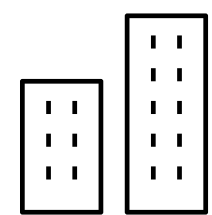
即使意识到数据安全的必要性, 很多公司也未配备专门负责保护敏感数据的人员。开展数据安全或审计活动期间, 当组织为找出责任人而承压时, 此情况通常会明显暴露。

高层管理人员可能会求助于首席信息官 (CIO), 而后者可能会表示: “我们的工作保持关键系统的稳定运行。去跟 IT 人员谈谈吧。” 这些 IT 员工可能会负责管理敏感数据所在的多个数据库, 但又缺乏网络安全预算。

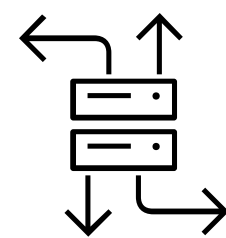
通常, 首席信息安全官 (CISO) 组织的成员不会直接负责流经整个业务的数据。他们可能会向企业内的不同业务线 (LOB) 经理提供建议, 但在很多公司, 无人专职负责管理这些数据。对于组织而言, 数据只是其最具价值的资产之一。然而, 如果缺少责任制度, 妥善保护敏感数据将成为一项挑战。



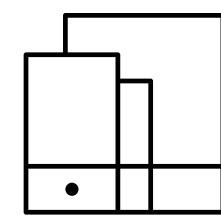
在复杂的 IT 环境中, 考虑以下位置的数据十分重要:



跨业务部门共享的数据



位于混合多云基础架构中的
数据



存储在移动设备上的
数据

■ 解决方案: 聘请 CDO 或 DPO 专门负责敏感和关键数据资产的稳健和安全

首席数据官 (CDO) 或数据保护官 (DPO) 可履行这些职责。事实上, 总部设在欧洲或与欧盟数据主体有业务往来的公司面临要求其配备 DPO 的 GDPR 规定。此先决条件认为: 敏感数据 (在本例中为个人信息) 的价值已超出使用该数据的 LOB。此外, 该要求强调了企业应配备专用于负责数据资产的作业角色。

选择 CDO 或 DPO 时, 请考虑以下目标和责任:

技术知识和商业意识

评估风险, 并制定非技术业务主管可理解的涉及适当数据安全投资的实际业务案例。

战略实施

按技术级别指导计划的实时, 从而应用检测、响应和数据安全控制措施来提供保护。

合规领导力

了解合规要求, 并清楚如何将这些要求映射到数据安全控制措施, 从而确保业务合规。

监控和评估

监控威胁态势并
度量数据安全计划的有效性。

灵活性和缩放性

知道何时以及如何调整数据安全策略, 例如通过集成更先进的工具, 在新环境中扩展数据访问和使用策略。

分工

与云服务提供商共同设定针对服务级别协议 (SLA) 的期望, 以及与数据安全风险和修复相关的责任。

数据泄露响应计划

最后, 准备好在制定战略性漏洞缓解和响应计划方面发挥关键作用。

最终, CDO 或 DPO 应带头促进各团队之间以及整个企业内的数据安全协作, 因为人人均需共同致力于有效保护公司数据。此协作可帮助 CDO 或 DPO 监督组织所需的计划和保护, 从而帮助保护其敏感数据。

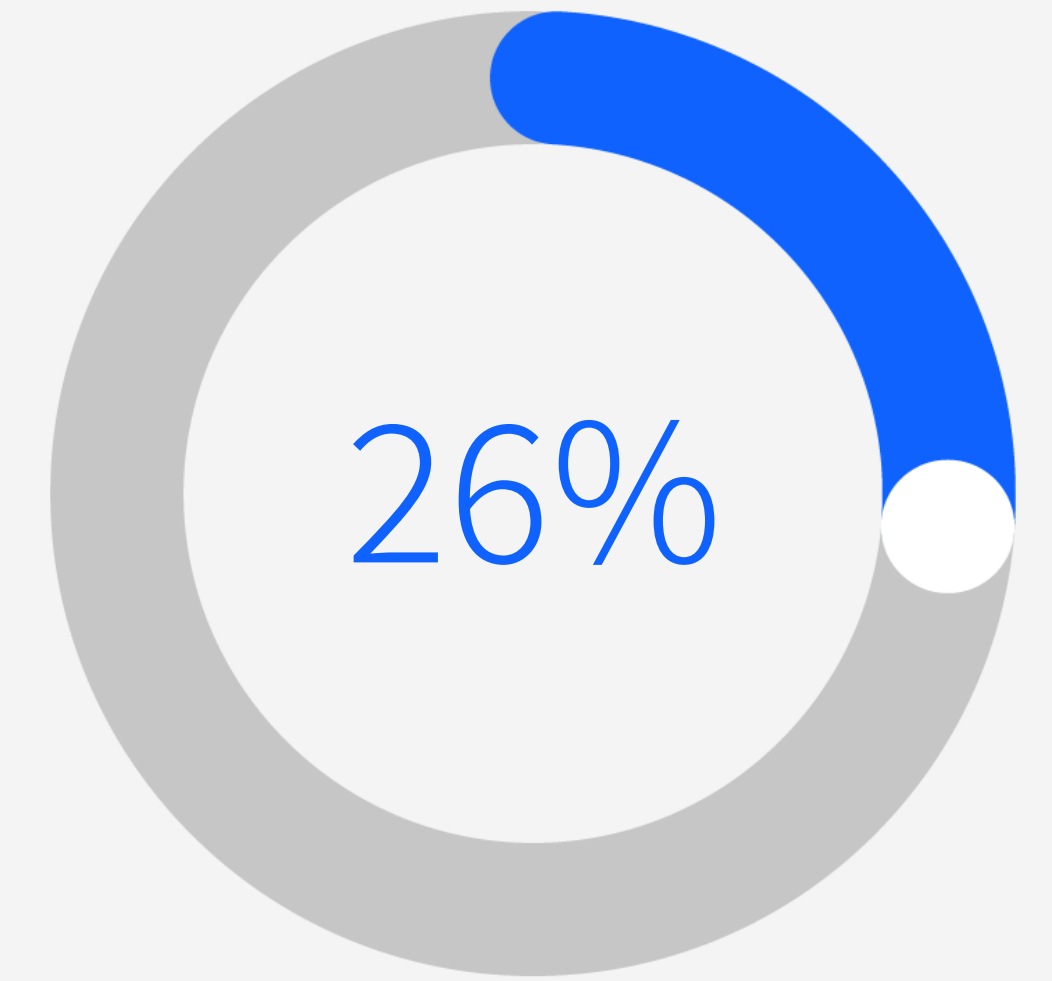


陷阱 4：未能解决 已知漏洞

企业中最引人瞩目的漏洞通常源于已知漏洞, 而此类漏洞即使在补丁发布后也仍未修补。未能快速修补已知漏洞会使组织数据面临风险, 因为网络犯罪分子会主动寻求此类唾手可得的入口点。

但很多企业发现, 碍于 IT、安全和运营部门之间所需的协调水平, 要快速安装补丁具有挑战性。此外, 补丁通常需进行测试, 以了解其是否不致中断流程或引入新的漏洞。

在云环境中, 有时很难知道是否应修补某一合同规定服务或应用程序组件。即使在服务中发现漏洞, 其用户通常也无法控制服务提供商的修复流程。



26% 的新漏洞已知先前被利用过。³

通过对数据存储进行漏洞评估来主动出击, 从而帮助降低风险。

■ 解决方案: 使用适当的技术制定有效的漏洞管理计划, 以支持其发展

漏洞管理通常涉及以下几个级别的活动:

- 维护数据资产的准确清单和基线状态。
- 对整个基础架构(包括云资产)进行频繁的漏洞扫描和评估。
- 优先考虑漏洞修复, 以便考虑漏洞被利用的可能性以及该事件对业务的影响。
- 将漏洞管理和响应度纳入与第三方服务提供商签订的 SLA 中。
- 尽可能加密敏感数据或个人数据。加密、标记化和编辑是实现此目标的三个选项。

- 采用适当的加密密钥管理机制, 确保加密密钥得到妥善存储并正确更新, 从而保障加密数据的安全。

即使在成熟的漏洞管理计划中, 也无法完全保护所有系统。假设在保护最完善的环境中也可能会出现入侵, 则表示您的数据需要更高级别的保护。正确的数据加密技术和功能集有助于保护您的数据免受新兴威胁的影响。

陷阱 5: 未能确定现代数据活动
监控的优先级并对其加以利用

陷阱 5: 未能确定现代数据活动监控的优先级并对其加以利用

监控数据的访问和使用是所有数据安全策略的重要组成部分。组织领导层需知晓数据访问的对象、方式和时间。此监控应包括相关人员是否应拥有访问权限、该访问级别是否正确以及它是否会给企业带来更高风险。

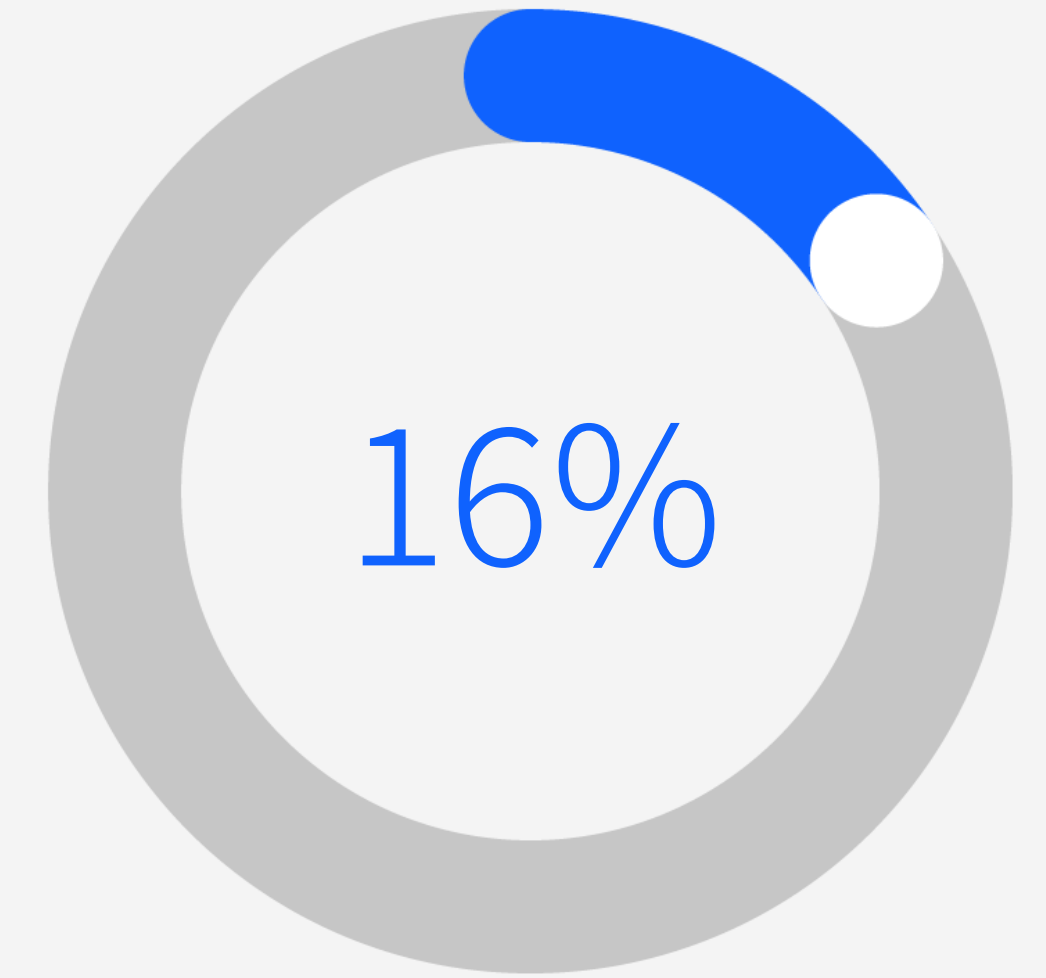
特权用户是内部威胁中常见的罪犯。数据保护计划应包括实时监视,以检测用于可疑或未经授权的活动特权用户帐户。

为防止潜在的恶意活动,解决方案须执行以下任务:

- 基于策略违例规定,屏蔽并隔离可疑活动。
- 基于异常行为,暂停或关闭会话。
- 在不同数据环境中使用特定于法规的预定义工作流程。
- 向 IT 安全和运营系统发送可操作警报。

考虑数据安全性和合规性相关信息并了解何时以及如何响应潜在威胁,这可能十分困难。由于授权用户访问多个数据源(包括数据库、

文件系统、大型机环境、云环境和 SaaS 应用程序),要保存所有这些交互的数据,可能是力不从心的。其中的挑战在于如何有效地监控、捕获、筛选、处理和响应大量数据活动。如果缺乏适当的计划,您的组织便可能会有超出合理处理能力的过量活动信息,从而削弱数据活动监控的价值。



在观察到的事件中,有 16% 存在滥用有效帐户的情况。在此情况下,对手会获取并滥用现有帐户的凭证以作为获取访问权限的手段。³

使用数据活动监控解决方案有助于数据安全分析人员节省宝贵时间。

■ 解决方案: 制定全面的数据安全性和合规性策略

为此, 在开启数据安全之旅时, 您需要调整监控工作的规模和范围, 从而妥善应对相关要求和风险。此活动通常涉及采用某一分阶段方法, 以便在整个企业中制定和调整最佳实践。此外, 在流程早期与关键业务利益相关者和 IT 利益相关者开展对话以了解短期和长期业务目标, 这一点也至关重要。

这些对话还应包括支持其关键举措所需的相关技术。例如, 如果您的企业计划在新址设立办事处, 并混合使用本地部署、云托管数据存储库和 SaaS 应用程序, 那么数据安全策略应评估该计划对组织的数据安全性和合规性状况有何影响。在此情况下, 公司拥有的数据此刻必须遵守新的数据安全性和合规性要求, 例如 GDPR、CPRA、巴西的 Lei Geral de Proteção de Dados (LGPD) 等。

您还应优先考虑可能包含最敏感数据的一两个来源。在将这些实践扩展到基础结构的其余部分之前, 请确保针对这些来源的数据安全策略足够清晰、详尽。

您应该寻找一种自动化数据或文件活动监控解决方案, 它具有丰富的分析功能, 可以重点关注特权用户引发的关键风险和异常行为。尽管在数据或文件活动监视解决方案检测到异常行为时接收自动警报至关重要, 但在发现异常或偏离数据访问策略时, 还须能采取快速措施。保护操作应包括动态数据屏蔽或阻止。

陷阱 5: 未能确定现代数据活动监控的优先级并对其进行利用

在制定数据活动监控和保护计划时, 考虑以下问题通常会有所帮助:

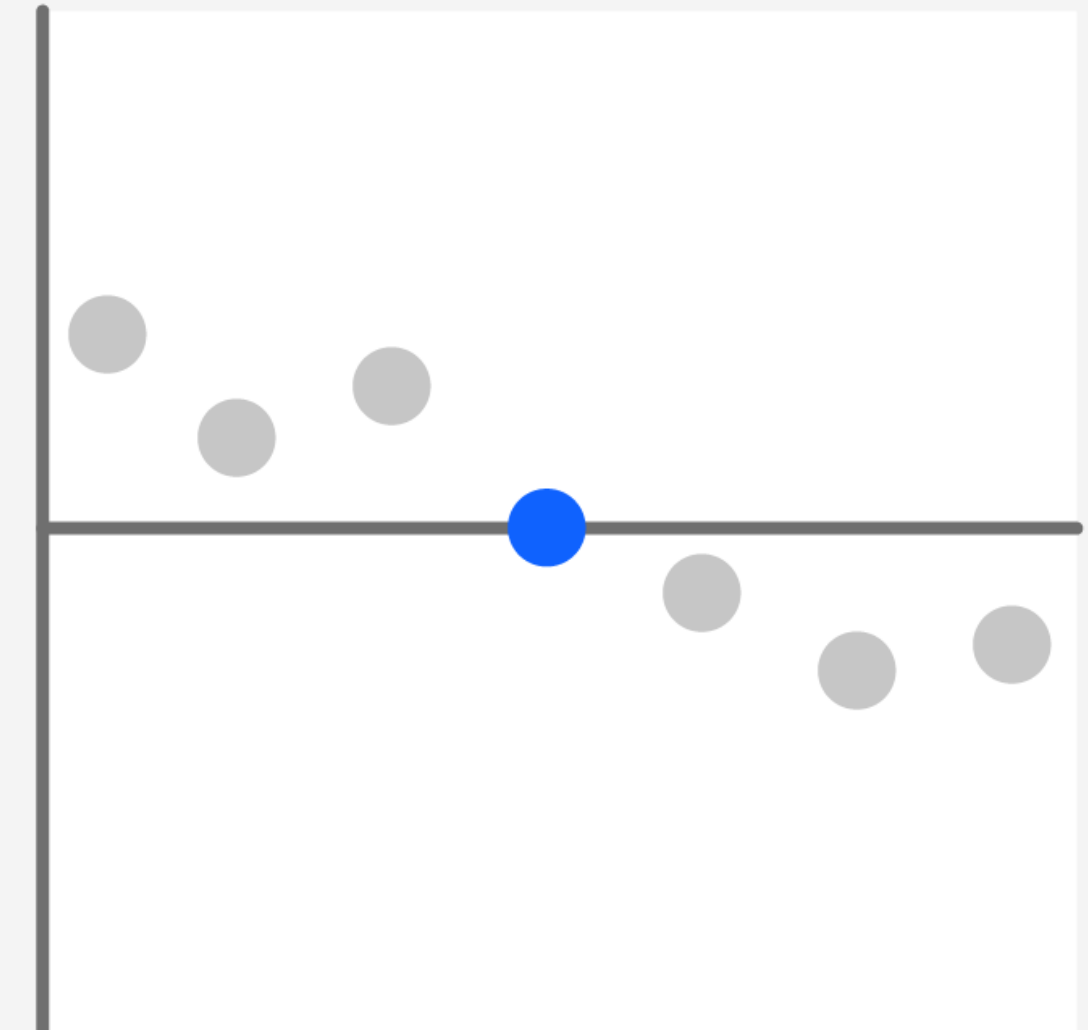
- 我最敏感的两个数据源是什么?
- 接下来, 我应根据敏感数据量优先处理哪五到十个数据源?
- 某些端点或云资产是否与高风险数据存在关联?
- 敏感数据是否可在本地、混合和云环境之间自由移动?
- 应在哪些条件下向哪些用户授予数据源的访问权限?
- 哪些高风险用户或特权帐户需关闭或需开展更严格的审查?

- 我的数据安全解决方案是否支持实时活动监控和自动化数据保护功能?
- 是否已部署实时监控以跟踪数据存储中所存储文件内的数据, 例如结构化查询语言 (SQL) 数据库和 Hadoop 发行版, 而不光是 SQL (NoSQL) 平台等?
- 我的监控解决方案是否考虑了跨混合多云环境的数据存储, 并允许我生成自定义报告, 以便在正确时间发送给正确人员?
- 我是否具备所需的风险分析和筛选监控功能, 以有效确定风险、漏洞和修复工作优先级?

监视优先级和保护要求越具体, 解决方案应用其可用检测与响应资源的效果就越出众。

176 万美元

与未广泛使用安全 AI 和自动化技术的组织相比, 广泛应用相关技术的组织平均节省了 176 万美元。²



后续应采取哪些措施？

如何避免这些常见的数据安全陷阱,尤其是在越来越多公司追逐混合多云环境的情况下?首先要认识到问题,并让组织做好准备,从而采取主动且全面的方法来保护数据,无论数据驻留在何处。

如果您的企业部署了复杂的混合 IT 环境,则无法依靠孤立的数据安全方法来保护数据。此时,您需要添加跨整个数据基础架构并支持所有数据类型的数据安全性和合规性策略。

为保护组织的宝贵数据,您可立即采取的后续步骤包括:

- 制定数据安全性和合规性计划,以支持组织的短期和长期业务目标与技术目标
- 用适当的人员、流程和工具实施该计划
- 规划资源,确保数据安全性和合规性计划可随组织采用现代化科技的步伐而有效调整

IBM® Security Guardium 平台是一套数据安全性和合规性解决方案,它旨在帮助组织采用更智能、适应性更强的方法来保护关键数据和敏感数据,而无论这些数据驻留在何处。了解为何它非常适合您的组织。

[了解更多信息](#) →

[联系我们](#) →



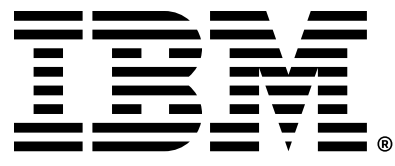
关于 Guardium 解决方案的一项研究发现,其在三年内的投资回报率为 406%,收益则为 586 万美元。⁴

为什么选择 IBM Security?

IBM Security 通过融入动态安全 AI 和自动化功能的集成安全性产品服务组合,帮助全球规模最大的企业和政府强化安全措施。该产品组合得到了世界知名的 IBM® X-Force® 研究的支持,使组织能够预测威胁、保护移动中的数据,并快速准确地应对威胁,同时不会阻碍业务创新。IBM 受到数千家组织的信赖,成为其评估、制定策略、实施和管理安全转型的合作伙伴。

IBM 管理和运营全球覆盖面最为广泛的安全研发与交付组织,每天在 130 多个国家/地区监测超过 1,500 亿次安全事件,已在全球范围内获得了超过 1 万项安全专利。





1. 2023 年数据泄露成本报告, IBM, 2023 年 7 月。
2. 当今云时代对数据合规性的需求, TechTarget 企业战略小组, 2023 年 4 月。
3. 2023 年 X-Force Threat Intelligence 指数, IBM Security, 2023 年 2 月。
4. IBM Security Guardium 数据保护的总体经济影响™ (TEI), IBM 委托 Forrester Consulting 进行的一项研究, 2023 年 6 月。

© Copyright IBM Corporation 2023

国际商业机器(中国)有限公司
了解更多信息, 欢迎访问我们的中文官网:
<https://www.ibm.com/cn-zh>
IBM Corporation
New Orchard Road
Armonk, NY 10504

美国出品
2023 年 9 月

IBM、IBM 徽标、Guardium、IBM Security 和 X-Force 是 International Business Machines Corporation 在美国和/或其他国家或地区的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。IBM 商标的最新列表可参见 [ibm.com/cn-zh/legal/copyright-trademark](https://www.ibm.com/cn-zh/legal/copyright-trademark)。

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

本文档内的信息“按现状”提供, 不附有任何种类的(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的协议条款和条件获得保证。

良好安全实践声明: 任何 IT 系统或产品都不应被视为完全安全, 任何单一产品、服务或安全措施都不能完全有效防止不当使用或访问。IBM 不保证任何系统、产品或服务可免于或使您的企业免于受到任何一方恶意或非法律行为的影响。

客户负责确保对所有适用的法律和法规的合规性。IBM 不提供任何法律咨询, 也不声明或保证其服务或产品确保客户遵循任何法律或法规。