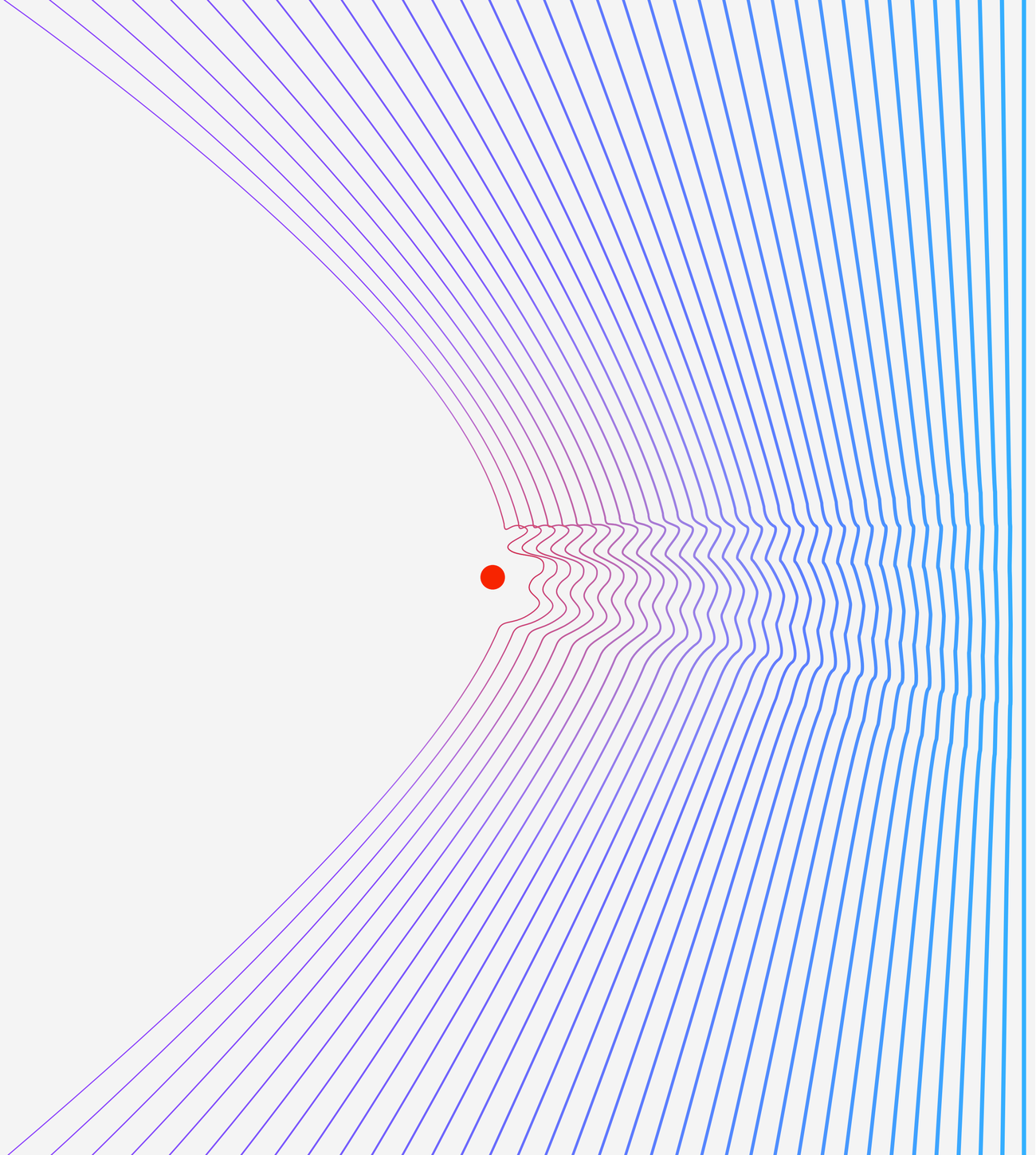
IBM **Security**

2023 年数据泄露成本报告



IBM

目录

01

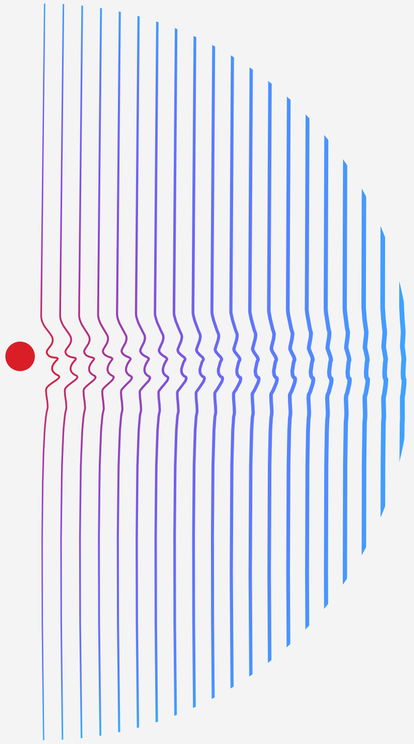
执行摘要

《数据泄露成本报告》为 IT、风险管理和安全主管提供了可量化的论据和佐证，以帮助各方更好地管理安全投资、风险情况和战略决策流程。2023 年版是该报告连续第 18 年发布的版本。

今年的研究由波耐蒙研究所 (Ponemon Institute) 独立进行并由 IBM Security® 发起、分析和发布，调研了 2022 年 3 月至 2023 年 3 月期间受数据泄露影响的 553 家组织。

本报告中提及的年份
是指报告发布的年份，
而不一定是泄露事件发生的年份。
所调研的泄露事件发生在
16 个国家和地区，涉及 17 个不同行业。

在本报告中，我们将研究数据泄露的根本原因以及短期和长期后果。我们还将探讨能让公司减少损失的各类因素和技术，同时避免采取那些会导致成本增加的因素和技术。



2023 年报告新增内容

每年，我们都会不断改进数据泄露成本报告，覆盖新出现的内容，以匹配新技术、新兴策略和近期事件。今年的研究首次探讨了：

- 如何识别泄露行为：无论源于组织自身的安全团队、其他第三方还是攻击者
- 执法部门参与抵御勒索软件攻击而产生的影响
- 勒索软件运行手册和工作流程的影响
- 与监管罚款相关的特定成本
- 公司是否以及如何计划因泄露而增加安全投资
- 以下缓解策略产生的影响：
  - 威胁情报
  - 漏洞和风险管理
  - 攻击面管理 (ASM)
  - 托管安全服务提供商 (MSSP)

随着泄露成本不断增加，本报告可为各方提供重要洞察成果，可帮助安全和 IT 团队更好地管理风险并限制潜在损失。报告分为五个主要部分：

- 介绍重要结论和 2023 年新增内容的执行摘要
- 对完整调查结论的深入分析，包括按地理区域和行业划分的数据泄露成本
- IBM Security 专家根据本报告的结果提出的安全建议
- 组织统计数据与行业定义
- 研究方法，包括如何计算成本

重要结论

本报告所述主要结论基于 IBM Security 对波耐蒙研究所 (Ponemon Institute) 所汇编的研究数据的分析而得出。本报告中成本金额的计量单位为美元 (USD)。

445 万美元

泄露的平均总成本

2023 年，数据泄露的平均成本达到 445 万美元，创下历史新高。相较于 2022 年的 435 万美元，该成本增加了 2.3%。拉长时间线来看，平均成本较 2020 年报告中的 386 万美元增加了 15.3%。

51%

因数据泄露而计划增加安全投资的组织所占比例

虽然数据泄露的成本持续上升，但报告参与者在是否因数据泄露而计划增加安全投资的问题上几乎各持己见。确定需要额外投资的首要领域包括事件响应 (IR) 规划和测试、员工培训以及威胁检测和响应技术。

---

176 万美元

针对数据泄露造成的财务影响，广泛采用安全 AI 和自动化可获得良好的效果

在识别并遏制安全泄露事件方面，安全 AI 和自动化被证明是能够降低成本以及缩短时间的重要投资。广泛采用这些功能的组织在识别并遏制泄露方面耗费的时间平均缩短了 108 天。报告还指出，与不使用安全 AI 和自动化功能的组织相比，数据泄露成本降低了 176 万美元。

1/3

组织自身的安全团队或工具发现的漏洞数量
仅有三分之一的公司通过自己的安全团队发现了数据泄露事件，这凸显了亟需更好的威胁检测手段。67% 的漏洞是由良性第三方或攻击者自己报告的。当攻击者披露漏洞时，相较于内部检测，组织会损失近 100 万美元。

47 万美元

未让执法部门参与抵御勒索软件攻击的组织所承受的额外成本
今年的研究表明，将执法部门排除在勒索软件事件之外会导致更高的成本。虽然 63% 的回应者表示他们的数据泄露事件有执法部门介入，但 37% 的回应者表示没有执法部门介入，却还是多支付了 9.6% 的费用，并且泄露生命周期延长了 33 天。

53.3%

自 2020 年以来，医疗数据泄露成本增加了 53.3%
自 2020 年以来，受到严格监管的医疗保健行业的数据泄露成本大幅上升。根据报告，医疗保健行业数据泄露造成的损失已连续 13 年位居榜首，耗费的平均成本高达 1,093 万美元。

82%

涉及存储在云端（公共、私有或多个环境）中各类数据泄露所占比例
2023 年，云环境成为网络攻击者的常见目标。攻击者通常会入侵多个环境，39% 的漏洞跨越多个环境，造成的损失高于平均水平，达到 475 万美元。