

# 安全保护始于内部—— 保护敏感数据远离内部威胁

首席信息安全官正在积极巩固其组织的边界防御，但如何才能应对企业内部已有的安全威胁？

**60%** 的攻击是由内部威胁造成的<sup>1</sup>

**61%** 的组织监视特权用户不比监视普通用户更严密<sup>1</sup>

**70%** 的组织没有支持权限报告的数据安全解决方案<sup>2</sup>

## 拥有敏感数据访问特权的员工 具有最大的风险



员工错误地打开恶意软件



心怀不满的内部人员蓄意造成危害



第三方损害敏感数据

### 如何才能缓解内部威胁？

#### 了解您的用户

谁有权访问敏感数据？  
用户和管理员使用该数据做什么？

#### 了解您的数据

哪些数据是敏感的？  
您能否控制特权用户对敏感数据的访问？

IBM® Security Guardium® 是一个全面的数据安全平台，提供了各种数据保护功能——从敏感数据的发现和分类到漏洞评估，再到数据和文件活动的实时监控。

**45%** 减少了发生违规的可能性<sup>3</sup>

**20%** 减少了花在安全与合规性上的时间<sup>3</sup>

获取该电子书，进一步了解 Guardium 如何帮助您保护敏感数据远离内部威胁。

下载该电子书



IBM、IBM 徽标、ibm.com 和 Guardium 是 International Business Machines Corp. 在全球许多司法管辖区的商标或注册商标。其他产品和服务名称可能是 IBM 或其他企业的商标。Web 站点 [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml) 上的“Copyright and trademark information”部分包含了 IBM 商标的最新列表。

<sup>1</sup> “IBM X-Force 研发团队 2016 年网络安全情报索引”

<sup>2</sup> “特权访问：管理潜在风险，保护数据安全 UBM Research。2016 年。”

<sup>3</sup> “IBM Security Guardium 的 Forrester 总体经济影响分析。”Forrester Research。