巧妙应对，消除内部威胁

借助 IBM 的智能化集成式安全解决方案，降低与内部人员有关的数据风险

IBM Security 白皮书

防御日益增长的可信内部人员威胁

安全漏洞屡屡见诸报端，这导致我们很容易认为所有敌人都来自企业外部。但是现实却很残酷：超过一半的攻击都是源自内部人员蓄意或无意的行为。[1] 换而言之，这些攻击很可能是由您信任的人发起的。这些威胁可能会给企业带来重大的经济损失或名誉损失。

60% 的攻击来自拥有内部访问权限的人。[1]

谁代表内部威胁？

在这种情况下，内部人员是指可以物理访问或远程访问公司资产的任何人。威胁可能来自：

- 不满的员工 - 他们决定泄露敏感信息，获取个人利益或进行报复
- 心怀恶意的员工 - 他们故意滥用对网络、系统或数据的访问权限，给企业造成损失
- 泄密的员工 - 他们无意识的行为导致系统遭受攻击或者他们犯下的错误导致恶意软件入侵（比如，点击了含有恶意软件的电子邮件，导致攻击者窃取了访问证书）
- 第三方（承包商、合作伙伴和客户）- 他们对敏感数据具有可信访问权限，也会带来以上几种的威胁

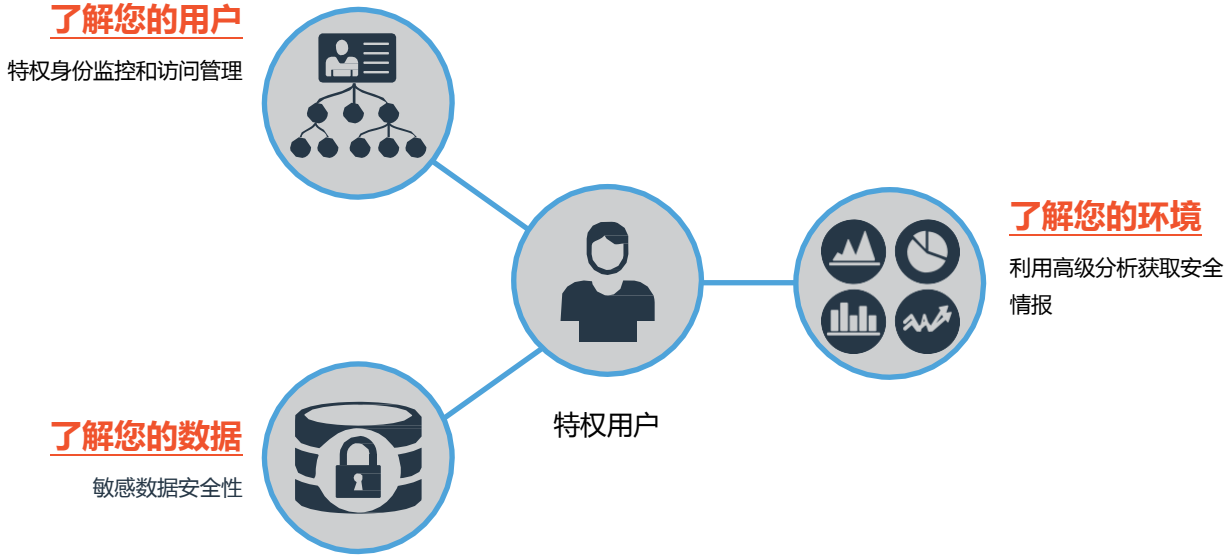
如何防御这些威胁？

向员工开展可疑通信和潜在风险的相关教育非常重要。但是，除此之外，您还需要能主动防御新兴内部威胁的集成式解决方案来提供支持。

[1] 《回顾年度严重数据泄露事件、大型攻击和新型漏洞》，IBM X-Force 研发团队：2016 年网络安全情报指数，2016 年 4 月.

从了解您的用户、数据和环境着手

为了防御内部威胁，您必须知道需要保护的对象以及由谁来保护这些对象。最大的风险来自特权用户，因为他们拥有对最敏感的资产的特殊访问权限。因此，您需要控制特权用户，监控敏感数据，并分析整个环境中的行为，以消除潜在漏洞。



61% 的企业并没有特别监控特权用户。[1]

[1] 《特权访问：管理潜在风险，保护您的数据》，UBM Report，2016 年 4 月.

着手行动：了解您的用户

面对内部威胁，即使是最信任的关系也不能想当然地认为他们不会带来威胁。特权用户在开展工作时，一方面您需要给予信任，另一方面，您需要核实特权用户的身份以及他们是否只访问了他们需要的信息。

IBM® Security Privileged Identity Manager 交付了一个集成式解决方案，该解决方案主要用于保护、监控和审核特权账户的使用。它的设计初衷是通过实现特权身份使用的自动化和审查，抵御内部威胁。该解决方案能集中管理和审核特权用户证书池，实现中央密码管理，从而保护企业资源免受内部威胁。

在了解用户和用户行为方面，IBM Security Privileged Identity Manager 能帮助您：

- 利用会话记录和回放支持，监控特权用户的行为
- 利用加密证书库，控制共享账户的签入和签出
- 不需要在应用内共享特权用户的证书和硬编码密码
- 利用强大的认证控制和单点登录功能，保护高危账户的访问
- 在企业内共享策略管理，交付经济高效的解决方案

了解用户时必须解答以下关键问题：

- **谁访问了敏感数据？**
- **谁应该访问敏感数据？**
- **最终用户利用数据做了什么？**
- **管理员利用数据做了什么？**

▶ 查看信息图表，了解如何借助 IBM Security Privileged Identity Manager，抵御内部威胁。

着手行动：了解您的数据

敏感数据是内部攻击者的一个重点目标。因此，不论敏感数据保存在何处，您都必须保护好这些数据。您需要采取恰当的安全措施来保护数据库、数据仓库、文件系统、大数据平台和云环境。同时，您还需要实时跟踪访问、发现异常情况，防止出现数据泄露。

IBM Security Guardium® 是一款综合的数据安全解决方案，能帮助您了解哪些人从何处访问了所有主要平台上的哪些敏感数据，以及他们访问的时间和方式。该解决方案旨在预防未经授权的行为或可疑的行为，以及敏感数据库中的漏洞，它能自动发现和归类敏感数据，并识别合规风险。此外，Guardium 还提供高级自动分析功能，来区分正常行为和异常行为，识别风险，帮助您实时采取行动，防止出现数据丢失。

在了解数据和缓解风险方面，Guardium 能够：

- 基于策略实时、持续地监控敏感数据库
- 扫描数据源，发现其中的漏洞（丢失的补丁、配置错误的特权等），帮助您加固环境，防止出现漏洞
- 防止数据、数据结构、配置文件和日志等出现未经授权的变更
- 分析数据，提前检测出攻击征兆，比如 SQL 注入和恶意程序
- 利用加密、隐藏、修订、拦截、警报和用户隔离功能，保护静态数据和动态数据
- 支持高级行为分析，实时提供可执行的保护措施，包括动态警报、数据隐藏和拦截，以及用户隔离

了解数据时必须解答以下关键问题：

- **哪些数据属于敏感数据，它们保存在何处？**
- **是否暴露了恰当的敏感数据？**
- **与敏感数据相关的风险有哪些？**
- **您能否控制特权用户对敏感数据的访问？**

查看信息图表，了解如何利用 Guardium，防御内部威胁。

着手行动：了解您的环境

为了提前发现威胁，您必须能够检测环境中的可疑行为，并采取行动。除了了解您的用户和数据外，您还需要利用分析功能来识别缓慢又不起眼的威胁，这类威胁可能会持续几个月的时间。同时，您还需要提醒安全团队快速做出反应。

基于 IBM QRadar® Security Intelligence Platform 的 IBM QRadar® Security Intelligence Platform 旨在实时监测威胁，并划分威胁的优先级。QRadar 能够将用户行为与日志事件、网络流量、威胁情报、漏洞和业务背景进行匹配，帮助您消除威胁。借助该解决方案，安全团队能够从冗杂的信息中找到清晰的信号，从而重点关注最迫切、最危险的威胁。此外，它还能指导安全团队采取缓解措施，将潜在损失最小化。

QRadar 集成了 Guardium、IBM Security Privileged Identity Manager 和其他解决方案中的数据，以便提供一种更智慧的内部威胁防御方法。QRadar 能够：

- 快速部署至整个网络，包括基于云的资源中
- 检测环境中的微小差别，比如潜伏者或怀有恶意的内部人员
- 收集、规范并关联数十亿事件，优先处理少量问题
- 发现重要的漏洞和风险，防止出现攻击
- 通过取证分析，支持您快速调查内部威胁

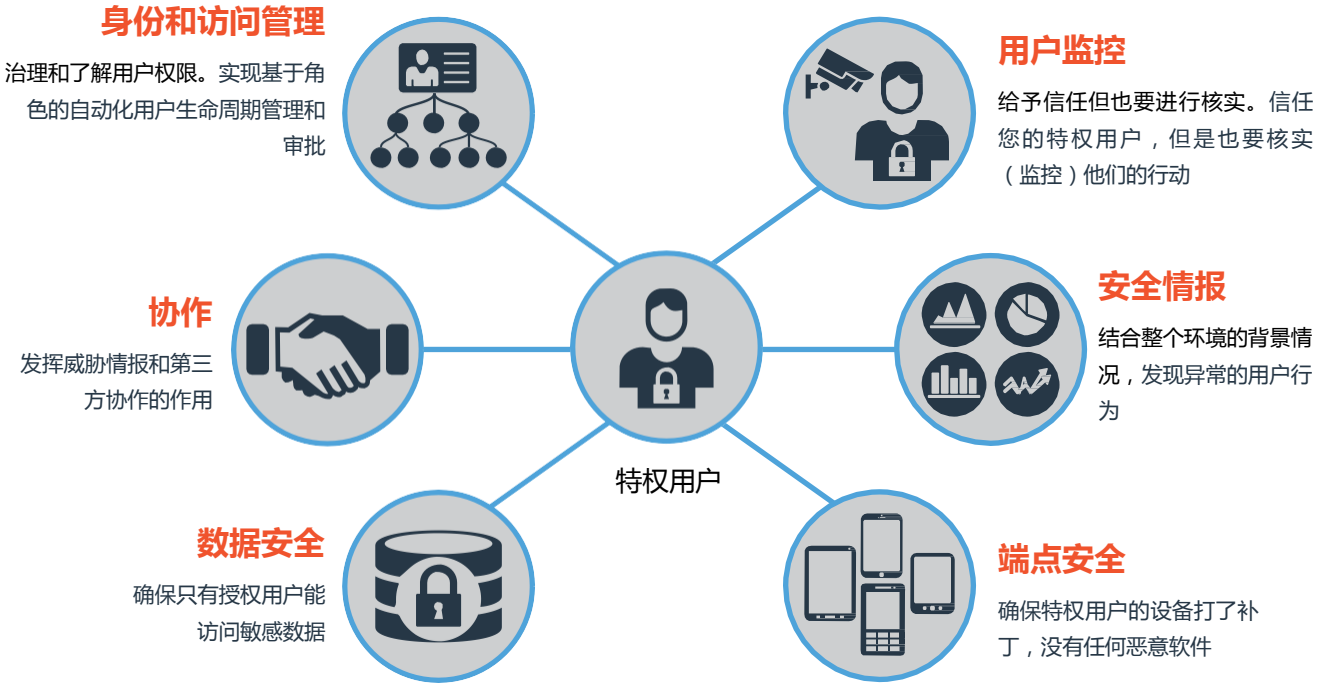
QRadar 帮助您巧妙地完成以下任务：

- **威胁检测**
- **风险评估与管理**
- **漏洞管理**
- **欺诈识别**
- **取证调查**
- **事件响应**

观看白板视频，了解如何利用 QRadar 分析解决方案，免遭攻击。

巧妙应对：多管齐下，实现全方位的强大保护

如今，以集成方式防御内部威胁变得比以往任何时候都重要。例如，结合利用用户监控工具和安全情报分工具，可提供审核用户活动和检测可疑行为的关键能力。有了所有网络行为和潜在系统漏洞的全方位视图后，安全团队就能提前发现威胁，在攻击实现之前拦截它。



81% 的内部攻击都使用了另一个人的证书来绕开控制程序或提高权限。[1]

1 《特权用户的滥用行为与内部威胁》，Ponemon Institute，2014 年 5 月.

巧妙应对：防范特权用户

通过集成身份和访问管理解决方案与数据安全解决方案，贵企业能够从正常行为中发现有意义的异常行为，并预防数据丢失。比如，当机密信息的访问、分配或下载出现异常时，您能够拦截和/或隔离相关的 ID。

IBM Security Privileged Identity Manager 和 Guardium 在保护共享 ID 的使用方面尤为有效。通过结合这两款解决方案，您能够在了解访问和数据活动的基础上提供不间断的实时数据保护，控制共享 ID 的访问和使用，防范特权用户的未授权活动或可疑活动以及来自外部的攻击。

IBM Security Privileged Identity Manager 和 Guardium 能帮助您：

- 核实可信用户的访问，持续监控对高价值数据资源的访问，比如数据库，大数据系统和文件系统等
- 验证共享 ID 获得的访问权限是否在界定特权范围内
- 发现使用通用服务 ID 访问数据的应用用户
- 评估授权用户是否向未授权用户披露或共享了证书

阅读本交互式白皮书，获取洞察力，了解如何抵御特权用户带来的威胁。

70% 的企业缺少支持授权报告的数据安全解决方案。[1]

[1] 《特权访问：管理潜在风险，保护您的数据》(Privileged Access: Manage the Potential Risk to Safeguard Your Data)，UBM Report，2016 年 4 月.

巧妙应对：把数据泄露扼杀在萌芽状态

为了帮助您防范泄露事件，IBM Security Guardium Threat Diagnostic Center 提供了专业的威胁检测分析功能，它能扫描和分析经过审查的数据，检测出正在发生的数据库攻击的征兆。Guardium 能够检测出来自企业内外部的 SQL 注入和恶意存储程序。比如，某个心怀不满的管理员利用存储程序掩盖重要表格的删除或表格内容的提取。

与某些解决方案不同，Guardium 不需要对照变化无穷的攻击特征字典，而是分析审查数据行为，寻找能代表 SQL 注入攻击或恶意存储程序的特定事件模式。这种方法更加灵活，且不需要持续更新攻击特征。相反，Guardium 能够与 QRadar 共享这些情报，而 QRadar 能借此生成更智慧、更有针对性的洞察力。

通过集成 Guardium、IBM Security Privileged Identity Manager 和 QRadar，您能够实时检测威胁，并划分威胁的优先级。这些解决方案能够自动关联事件，检测异常情况，相互共享信息，从而帮助您快速响应最危险的威胁。

- 阅读本白皮书，了解如何利用集成式安全情报，保护关键数据。
- 获取电子书，进一步了解如何保护敏感数据抵御外部威胁。

部署 Guardium 后，企业发现数据泄露的几率降低了 45%。[1]

[1] 《IBM Security Guardium 的总体经济影响力》(The Total Economic Impact of IBM Security Guardium)， Forrester Research，2015 年 9 月.

巧妙应对：下一步

数据安全、身份和访问管理措施以及安全情报就位后，贵企业就拥有了抵御外部威胁的强有力保障。但是，集成式 IBM Security 解决方案组合能够帮助您进一步检测威胁，遵守相关政策和法规，节约整个企业的成本。

您可以将以下解决方案纳入考虑范围：

- IBM BigFix® 端点安全 - 让您能够持续监控所有端点（从笔记本电脑、台式电脑、服务器到销售点设备），发现潜在威胁，贯彻安全合规措施，实时了解情况，从而应对事件
- IBM Security Identity Governance and Intelligence - 将合规、业务和 IT 角度意见相结合，对用户访问权的设计、审查和验证流程进行了简化，从而帮助减少访问策略违例现象
- 通过 IBM X-Force® 和 IBM Security App Exchange 展开协作 - 利用威胁情报和与业内同行的合作，划分情报事件的优先级，获取全面的洞察力

借助 IBM Managed Security Services，您能够利用业内领先的工具、安全情报和专业知识，提升您的安全状态，而且只需要花费一点点内部安全资源。

集成式 X-Force 威胁情报能为您提供快速发现和消除威胁的相关背景。

IBM 解决方案齐发力，解决内部威胁

IBM Security 解决方案，包括 Guardium、IBM Security Privileged Identity Manager 和 QRadar，是全球企业实现综合、分层的数据和网络保护的信赖之选。通过结合利用这些解决方案，您能够加大保护力度，防御所有类型的内部人员，同时降低总体复杂性和总体拥有成本。它们可以分析之前的漏洞模式，预测潜在的攻击领域；挖掘员工系统行为，识别各种潜在的滥用模式；并监控外部环境以发现潜在的外部威胁。

IBM 在多个安全产品领域内提供集成式解决方案，帮助客户实现这些解决方案功能的价值。具体来说，您能够获得：

- 集成式情报 - 关联和分析来自数百个信息源的孤岛式信息，自动检测和应对威胁
- 集成式保护 - 借助能跨领域交互、提供紧密结合且易于管理的保护的解决方案，提高安全性
- 集成式研究 - 融合有关漏洞、漏洞利用和恶意软件的最新信息，帮助您提前防范出现的威胁和风险

作为企业的战略合作伙伴，IBM 帮助企业在极度复杂的 IT 环境中减少安全漏洞，管理风险。

企业平均需要 158 天才能发现无意中造成的数据泄露。[1]

- 访问产品网页，进一步了解 Guardium。
- 访问产品网页，进一步了解 IBM Security Privileged Identity Manager。
- 访问产品网页，进一步了解 QRadar。

[1] 《2015 年数据泄露成本研究：全球分析》，Ponemon Institute，2015 年 5 月.

有关更多信息

如欲了解有关如何通过集成式的 IBM Security 解决方案防范内部人员威胁的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：**ibm.com**/security

IBM Security 简介

IBM Security 可以提供最先进的集成式企业安全产品和服务组合。该组合由世界知名的 X-Force 研究所提供支持，可提供一流的安全智能，帮助组织全面保护其基础架构、数据和应用，所提供的解决方案涵盖了身份和访问管理、数据库安全、应用开发、风险管理、终端管理、网络安全等诸多方面。这些解决方案可以帮助企业有效管理风险，为移动、云、社交媒体和其他企业业务架构落实集成安全。IBM 作为世界上覆盖范围最广的安全研究、开发和交付企业之一，每天对 130 多个国家/地区的 130 亿个安全事件进行监控，并拥有 3,000 多项安全专利。

此外，IBM 全球融资部可帮助您以最具成本效益及战略性的方式获得贵企业所需的软件功能。对于可信的客户，我们可以定制一款适于贵企业业务和发展需求的财务解决方案。IBM 全球融资部助您规划关键 IT 投资并推动企业发展。有关更多信息，敬请访问：**ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

美国印刷
2016 年 6 月

WGW03222-CNZH-00