金融服务：利益诱人的网络犯罪目标[1]

尽管金融行业在威胁监控和检测方面投入巨资，但黑客并未因此止步，不断对准关键数据源实施新的攻击手段。客户的财务数据和身份信息价值极高，可以在暗网上轻松变现，因此日渐成为勒索赎金的新目标。

攻击形式日益严峻，越来越具有破坏性

2 亿
— 在一年内遭泄露的财务记录数[2]

1.02 亿
— 金融企业经历的安全事件的数量[2]

65%
— 金融服务行业的安全事件要比其他行业多出 65% 以上[2]

42%
的金融服务攻击来自外部[1]

362 万美元
— 一次数据泄露的平均总成本[3]

8,100 万美元
— 通过银行账户盗用而被窃取的金额[2]

58%
为内部攻击[1]

53%
的安全事件由无心之失导致，但意外成为攻击者的帮凶[1]

5%
的安全事件由蓄意破坏的内部恶意人员引发[1]

[1]IBM X-Force 威胁情报索引，2017 年。[2]IBM X-Force 研究：2017 年金融服务业安全趋势
[3] “2017 年数据泄露成本调研，全球分析”，由 IBM 赞助，由 Ponemon Institute 执行；2017 年 6 月。

防范资产和客户损失的 5 大秘籍

1 **充分发挥分析和情报的力量**
自动捕获和使用网络威胁情报，通过机器学习和行为分析加强检测和预防能力

2 **部署数据安全和隐私措施**
增强数据保护、访问控制和监控，满足日益增长的监管、风险与合规控制的需求

3 **改善混合云安全与访问控制**
降低云风险，消除 IT 碎片化，充分发挥互操作性和云计算的效率

4 **建立物联网和移动安全措施**
满足不断增长的客户需求：支持随时随地通过任何设备进行访问，同时保障身份和财务数据的安全，防范跨渠道网络犯罪

5 **确保部署新技术**
主动检查潜在漏洞，发现为保持安全性和竞争优势所需的安全变更，包括区块链

采用 IBM® X-Force® 安全监控解决方案的企业，**安全事故减少 48%** [1]

了解如何保护贵企业，避免成为网络攻击的受害者。
认识 IBM Security，立即开始构筑您的防御系统。
请访问 **ibm.com**/security/solutions

SE912364-CNZH-01