

# IBM SECURITY BANKING SOLUTION

## IBM 金融业安全解决方案



### 行业需求概述

银行业对金融信息保护工作是基于行业和客户的基本要求。因为金融机构数据泄漏事故频发、信息安全无法保障，将会造成金融机构的客户流失、声誉受损、罚金等严重后果。金融IT安全包括了安全分析、人员安全、数据安全、应用安全、基础架构安全等多个领域，需要通过多个系统在多个领域的分工协作实现合理的信息安全保护。而目前很多银行的安全措施和系统，还不能完全达到银行和客户的要求，各种银行安全事件也缺少统一有效的集中管理和分析平台。

### 解决方案概述

IBM的安全框架包含5个领域：安全智能分析、人员安全、数据安全、应用安全、基础架构安全(包括网络安全和终端安全)，是一个结合了信息安全相关规范以及行业法规要求，并通过多年的实践、总结和整理形成的最佳实践方法论。



- **安全智能分析:** 通过自动化手段广泛地收集各种安全信息，包含了系统日志、网络活动、虚拟环境活动、用户登录和访问活动，及应用程序活动等，使安全专业人员其能够侦测其整个网

络内的各种潜在攻击源，对攻击之前、攻击期间、攻击之后进行的全方位的影响分析，以便更好地划定系统保护的优先级并做出响应预案。

- **人员安全管理:** 通过所有安全域的端到端身份信息管理，拓展企业级身份信息的关联。包括身份管理、安全登录管理等。如：
  - \* **特权身份管理:** 统一的用户管理平台；特权账号的使用通过流程进行控制；实现B/S、C/S应用的单点登录；实现应用的强认证保护，如客户端证书；用户对应用使用的监控和统计。
  - \* **账号集中管理和应用单点登录:** 用于构建企业用户身份账号管理平台，实现可靠的账号供给，帮助用户实现完整的员工账号的全生命周期的管理平台，覆盖员工和入职、调任、离职等各个阶段的需求。也可支持联邦内用户身份的管理。实现针对B/S和C/S结构应用的单点登录。提供IBM安全规则管理平台，实现基于应用的超细粒度应用权限管理。
- **数据安全:** 作为企业级解决方案，确保银行数据中心的可靠信息的隐私要求和完整性要求。包括数据库安全审计、密钥的全生命周期管理等。
  - \* **数据库安全审计:** 用于帮助客户对企业范围内所有数据库类型建立统一的数据库访问操作与行为的监控手段，能够在不影响数据库自身性能的情况下，对所有数据库行为实施基于安全规则的监控、过滤与报警，并提供基于数据库的自动化审计和生成合规报表的能力。除此之外，还提供数据库漏洞检测、评估与集中管理等能力。

# IBM SECURITY BANKING SOLUTION

## IBM 金融业安全解决方案

- **网络入侵防护系统:** 提供对用户数据、系统和关键应用程序的侵入、拒绝服务(DoS)、恶意代码、后门、间谍软件、对等应用程序以及一系列日益增加的混合威胁危害的风险缓解战略, 实现对恶意代码、流量的自动阻断。对现有的网络防护提供安全的、可管理和可扩展的整合平台(包括网络IPS、Web应用程序防火墙、虚拟化和数据泄露)。

### 解决方案价值主张

IBM的安全解决方案非常完整地覆盖了企业安全的各个方面, 可以满足客户对于安全的要求, 也通过集成和分析为企业的安全要求提供了完整的视角。

- **安全智能分析:** Gartner综合排名第一。工具开箱即用, 提供软硬一体化的解决方案, 见效快。提供覆盖网络7层的流量分析、威胁探测和取证。分布式数据结构, 实现高性能和高度的可扩展性。提供很强的用户登录和活动分析能力。
- **特权身份管理:** 是市场领先解决方案, 在国内银行和运营商拥有大量成功案例, 稳定性及可靠性得到充分验证, 具有超强集成能力、和应用松耦合、对应用改造量小的优势。
- **账号集中管理和应用单点登录:** 提供最为全面的操作系统平台的支持, 支持AIX、HP-UX、Solaris、Windows、Linux等主流的操作系统。拥有极为丰富的接口, 可以对几乎所有的应用系统进行用户帐户信息的集中管理和应用法单点登录。支持多种认证方式, 包括用户名密码、数字证书、RSA动态令牌、IP地址、EAI。提供了功能强大的安全审计功能, 包括账户状态、账户的使用情况、账户访问应用系统等。
- **数据库安全审计:** 业界排名第一的专业化数据库安全审计监控解决方案, 数据操作信息保存完整, 审计颗粒度细。数据操作

信息查询简易, 生成审计报告效率高, 易实施。作为企业级的解决方案, 拓展性非常高, 提供统一部署安全策略和报告汇总, 覆盖信息采集、解析、存储、查询、及工作流管理等功能, 国内已有大量案例。

- **网络入侵防护系统:** 是市场领先的解决方案, 是首个获得NSS评测连续五年Golden Award的厂商。依靠其强大的X-FORCE研发团队, IBM IPS客户可获得更优先、更安全的保护全产品线: 可以保护200 Mbps至23 Gbps的吞吐量不受未知威胁的影响。对服务器, 客户端提供虚拟补丁, 防止对操作系统及客户端应用程序漏洞的攻击威胁。提供Web应用程序及VMWare虚拟机防护。

### IBM软件产品

- QRadar(安全智能分析)
- Privileged Identity Manager(特权身份管理)
- Tivoli Access Manager(账号集中管理和应用单点登录)
- Network Intrusion Protection System(网络入侵防护系统)
- Guardium (数据库安全审计)
- zSecure (主机系统安全和审计)

### 典型业务场景

- 安全分析
- 身份管理
- 帐号管理与单点登录
- 数据库审计
- 网络入侵管理

© 版权所有IBM Corporation 2013

IBM、IBM徽标、ibm.com是国际商业机器公司在美国和/或其他国家或地区的商标或注册商标。如果上述和其他IBM商标在本文档中初次出现时带有商标符号(®或™), 则表示在此信息发布时, 这些商标是IBM拥有的、在美国的注册商标或普通法商标。此类商标在其他国家/地区也可能是注册商标或普通法规定的商标。可在网络上获取IBM商标的最新列表, 请查看[ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)的“Copyright and trademark information”部分。未经IBM公司书面许可, 不得以任何方式复制或传播本文档的任何部分。

到发布之日止, 产品数据都进行了准确性审核。产品数据可能随时更改, 恕不通知。关于IBM未来方向或打算的声明仅代表IBM的发展目标, 如有变更, 恕不另行通知。IBM“按原样”提供本出版物, 不进行任何明示或暗示的保证, 包括推销期间或出于某种目的而做出的任何暗示的保证。一些法律法规不允许在不预先通知的情况下在某些交易中表达或暗示质量免责声明。

本文档中针对IBM和非IBM产品及服务的性能数据是在特定的操作和环境条件下得出的。由任何该产品或服务的执行方获得的实际成果取决于大量特定于该方操作环境的因素并可能有很大差异。IBM不保证此类产品或服务的任何实现能够获得或包含此类成果。本文档中包含的有关第三方的任何材料基于从该方获得的信息, 并没有独立验证信息的精确性。本文档不等于来自IBM对任何第三方产品或服务的明示或暗示的建议或认可。

客户应自行保证遵守法律法规要求。获取有能力的法律顾问关于确定和解释任何可能影响客户的业务的相关法律和法规要求, 以及读者为遵守法律可能必须采取的任何措施的建议是客户自己的责任。IBM不提供法律建议, 也不表示或保证其服务或产品将确保客户遵从任何法律或规定。

