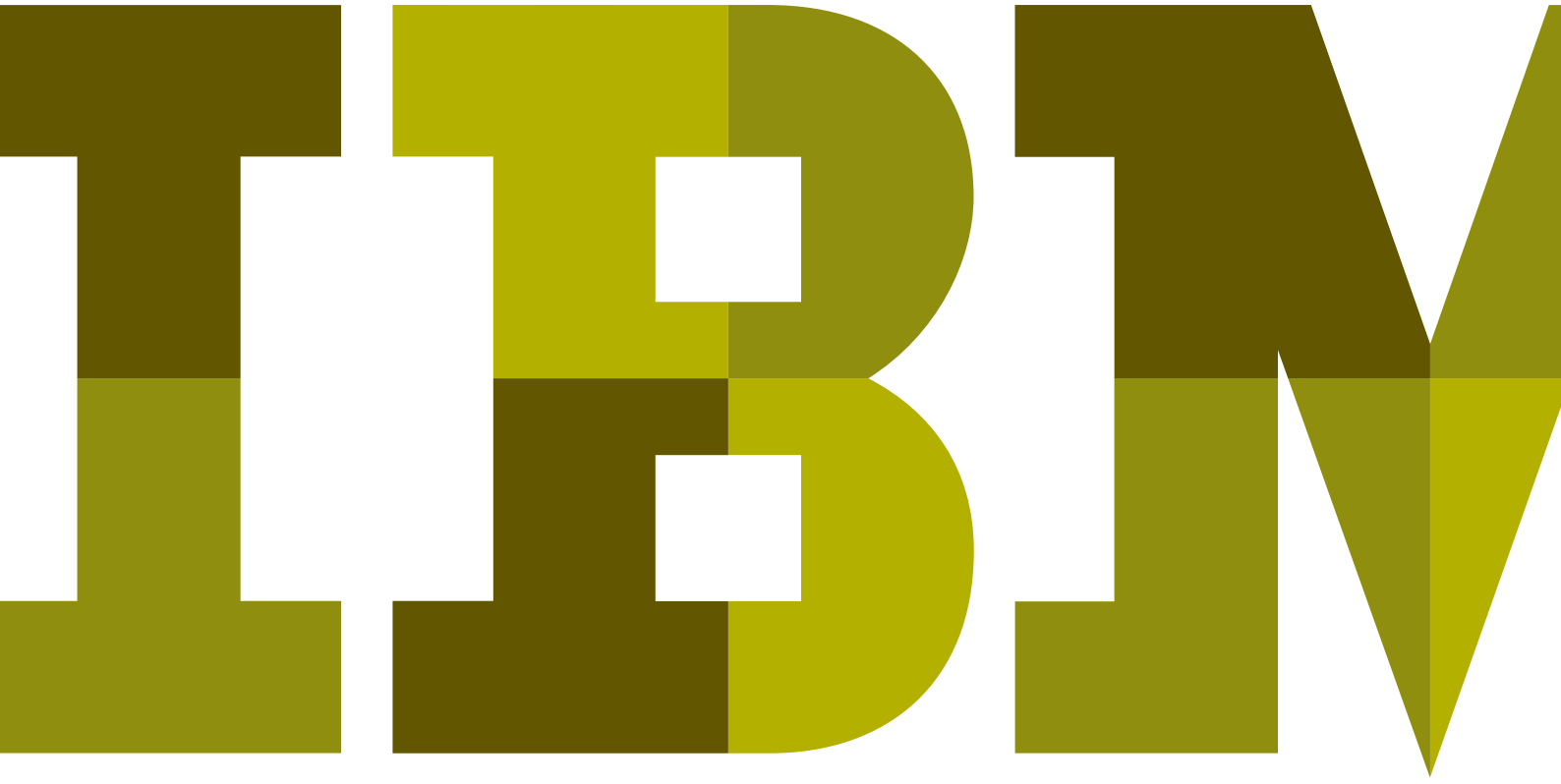
IBM软件

IBM安全产品: 智能、集成、专长

一个适合任何环境(从移动、云、社交到未知的未来)的综合框架

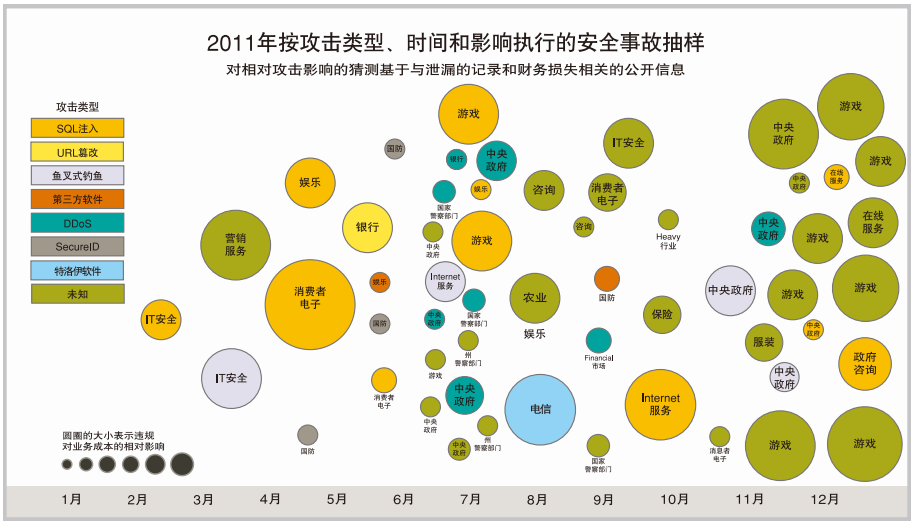


目 录

一个超级互联的商业世界

在如今超级互联的商业世界中，需要一种完全不同的方法来保障企业安全。激增的数字业务信息存储在消费者和企业所使用的虚拟云和社交平台、仪器、移动设备中，且可供访问，这就创造了一个极其复杂的IT环境——可能的攻击点几乎是无限的。

最有经验的对手现在正带来高级持续性威胁，他们通过密切的关注的坚持不懈来获取敏感业务信息的访问权限。这些攻击利用尖端的方法，可持续无限长的时间且具有专门的目标。如今，愈加多样的威胁侵蚀着传统IT防御(比如防火墙和防病毒软件)的有效性，甚至在许多情况下完全避开了这些控制。我们亟需一种新的方法，这种方法要在保护与检测、先进的技术与成熟的流程之间保持均衡。



作为IBM X-Force研究和开发团队所谓的“安全违规年”，2011年的主要特征是极大量的严重且多种多样的安全攻击。

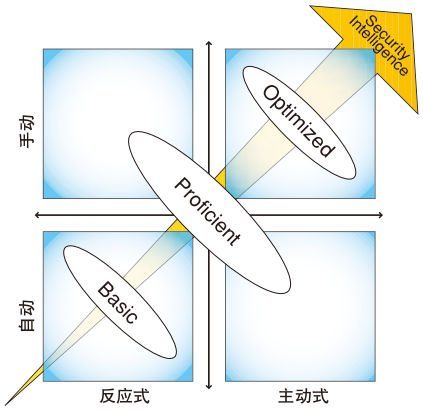
面向新世界的安全智能

只有公司部署了可监视、关联并分析从一个全面、集成的安全基础架构，以及经过深入研究的外部威胁源生成的海量实时事件的解决方案，才有能力经济高效地保持极强的安全态势。IBM将此称为安全智能。除了帮助检测和修复可能遗漏的漏洞，这种方法还让组织能够:

- 从反应性状态转向一种与业务目标更一致的主动式的方法
- 让业务人员能够比平时更快地部署创新计划
- 自动完成各种合规性活动
- 减少安全操作的人员需求

一种独有的综合方法

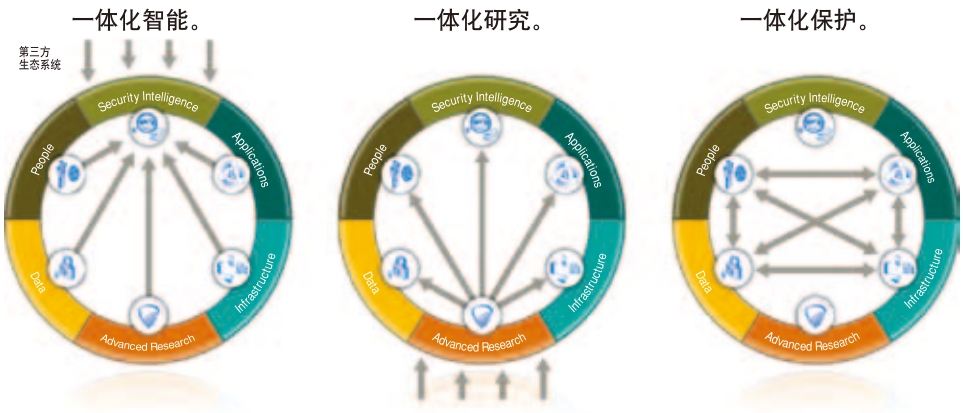
借助跨市场领域的领先产品和服务，以及基于3个主要原则(智能、集成和专长)的总体战略，IBM正帮助其客户实现真正的安全智能。



从反应式的手动方法转向主动式的自动化方法，这为组织带来了一种基于安全智能的且优化的安全态势。

智能

人类的智慧需要知识、信息，以及分析此信息以得出结论的能力。在企业安全领域中，这就需要具备相关网络和基础架构的可见性，以



安全智能、X-Force研究与核心保护资产的集成帮助填补了单点产品方法留下的覆盖空白。

及外部威胁智能，以及实时关联和分析功能，以识别和纠正可疑的活动。IBM Security提供了以下功能:

- **内部可见性:** IBM安全智能解决方案实时分析来自IBM产品和非IBM产品的信息。这些解决方案提供了跨所有4个安全风险区域的全面分析和洞察: 人员、数据、应用程序和基础架构。
- **外部威胁可见性:** IBM® X-Force® 威胁智能源提供了来自全球最大型的威胁和漏洞洞察存储库之一的关键信息，并以每天对130亿个安全事故的实时监视为基础。此洞察可识别可能与高级持续性威胁和广泛的对手相关的行为。
- **大数据时代的精准分析:** IBM安全智能解决方案可下钻到各个数据元素，以分析和查询各种不同的活动。这些解决方案提供了外围设备、外部云服务和移动设备上的网络访问，企业核心处的数据库活动，以及介于二者之间所有事件的洞察。

集成

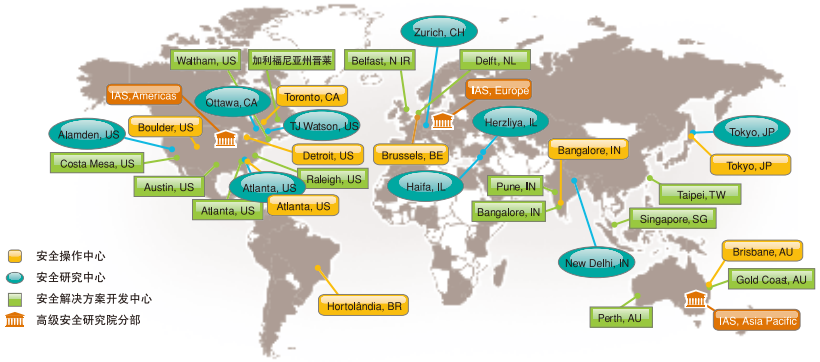
全面的IBM安全智能产品组合、X-Force研究与核心保护资产相集成，有助于减少通过打补丁拼揍成的安全单点产品中出现的可攻击弱点。

这种集成还可以简化部署，瓦解数据孤岛，从而简化合规性报告和改善安全智能，减少复杂性，并降低保持一种强大的安全姿态的成本。其他能节省成本和改善安全的功能包括:

- 用于漏洞检测、预测和修复的外部和内部上下文信息
- 已研究漏洞的自动化设备和软件更新
- 将身份验证和授权与可疑的数据库活动相链接
- 自动化的合规性和风险评估活动

专长

IBM拥有5,500多名研究人员、开发人员和主题专家参与安全计划，并运营着一个全球最大的企业安全研究及开发和交付组织。其中包括屡获殊荣的IBM X-Force研究和开发团队，以及一个业界最大的漏洞数据库、9个安全操作中心、10个IBM安全研究中心、15个安全解决方案开发实验室，以及在美国、欧洲和亚太地区拥有分部的高级安全研究院。IBM目前每天为130多个国家的客户监视着超过130亿个安全事件。

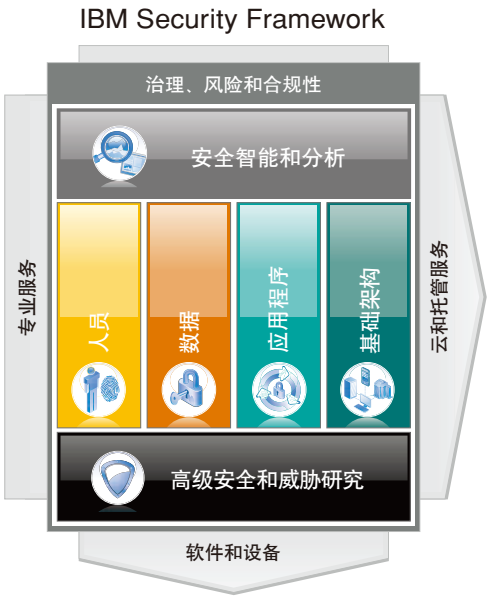


IBM运营着全球最大的安全研究及开发和交付组织。

IBM拥有各种顾问和专家，可帮助任何公司实现具有安全智能的优化、集成的安全控制。

产品组合

IBM Security Framework旨在帮助您确保正确的人能在正确的时机访问正确的资源，这样关键数据就可在移动和静止时受到保护，还可识别新兴的威胁以支持漏洞预防和修复，以及跨所有IT资源提供保护。这种集成的企业安全方法包含设备、软件产品和托管服务，并通过技术和风险咨询与实现服务来提供。但是，位于最核心位置的还是IBM产品组合。



IBM Security Framework提供了一种井然有序且高效的方法来满足安全需求，并满足整个企业的安全挑战需求。

安全智能和分析

全方位的视图

帮助预防、检测和修复安全漏洞与合规性风险。

挑战和解决方案要点

IBM安全智能产品能帮助您:

- **检测高级威胁:** 为自己配备全面且准确的安全智能。
- **解决合规性问题:** 自动完成用于审计和风险评估的数据收集和报告。
- **检测内部威胁和欺诈:** 在上下文内识别并理解可疑的用户活动。
- **预测企业面临的风险:** 主动识别安全漏洞和差距并确定优先级。
- **整合数据孤岛:** 在一个集成解决方案中收集、关联和报告数据。

产品

基于下一代安全信息和事件管理(SIEM)与日志管理的集成的安全智能产品家族包括:

- IBM Security QRadar® SIEM: 安全信息和事件管理，包括日志管理、威胁管理与合规性管理；复杂的事件和网络流关联；以及集成的行为分析和网络异常检测
- IBM Security QRadar Log Manager: 交钥匙式日志管理，开箱即用地支持数百个数据源，提供了预先打包的报告、仪表板和轻松的自定义功能
- IBM Security QRadar Risk Manager: 安全配置监视和审计；预测性威胁建模和仿真，以及高级威胁可视化和影响分析
- IBM Security QRadar Network Anomaly Detection: 网络流量异常检测，以及安全和网络数据的实时关联，旨在增强IBM Security SiteProtector™ System

- IBM Security QRadar QFlow and VFlow Collectors: 集成的网络流量收集和内容捕获，包括第7层应用程序分析，同时适用于物理和虚拟环境

控制、监视和验证用户对受保护数据和应用程序的访问。

挑战和解决方案要点

IBM Security身份和访问管理产品帮助您:

- **管理用户及其访问权限:** 在整个生命周期内高效地登记、管理和终止用户配置文件和访问权限。标记过期的帐户和角色冲突。
- **简化/跟踪用户对受保护资源的访问:** 集成生命周期访问权限与单点登录和密码管理，以及访问审计和报告。支持对设备执行强身份验证，以实现额外的安全性。
- **保护云、移动和软件即服务环境中的访问:** 为用户配备、基于角色的访问和联合身份提供一项通用的身份服务。集中进行用户授权和策略的安全管理。

产品

控制用户在整个生命周期内的访问活动和特权的集成解决方案包括:

- IBM Security Identity Manager: 从创建到终止的整个过程中管理用户帐户、访问权限、许可和密码
- IBM Federated Identity Manager: 以用户为中心、联合的单点登录，实现在受信任的业务合作伙伴之间共享信息，并简化跨分布式门户和大型机环境的应用程序集成
- IBM Security Access Manager for Web: 高度可扩展的用户访问管理和Web应用程序保护，用于防御高级威胁
- IBM Security Access Manager for Cloud and Mobile: 使用联合的单点登录(SSO)、用户身份验证和风险评分将用户访问保护扩展到移动和云环境
- IBM Security Access Manager for Enterprise Single Sign-On: 集成的身份验证、访问工作流程自动化、用户切换和审计报告，可帮助简化和加强访问安全
- IBM Security Identity and Access Assurance: 通过便捷的单点登录，针对企业应用程序和资源管理用户帐户、访问权限和密码

帮助保护各个关键控制点的关键数据资产，同时不影响生产力。

挑战和解决方案要点

IBM数据安全产品帮助您:

- **预防数据违规:** 监视各种事务，无需更改数据库或应用程序。创建逼真的测试集，同时屏蔽掉敏感的数据值。加密受监管的数据以帮助防止丢失—尤其是通过盗窃备份和媒介带来的丢失。以表单或文档形式编辑独立的或嵌入的非结构化敏感数据。
- **维护敏感数据的完整性:** 将所有事务与策略进行对比，并实时拦截各种违规。
- **降低合规性成本:** 自动化和集中化的控制，以简化合规性验证。

产品

IBM InfoSphere® Guardium® 产品旨在帮助确保数据中心内受信任信息的隐私性和完整性，这些产品包括：

- IBM InfoSphere Guardium Database Activity Monitoring: 一个简单强大的解决方案，帮助防止数据库和文件中的敏感数据泄漏，维护数据中心内的信息完整性，以及自动完成跨异构环境的合规性控制
- IBM InfoSphere Guardium Vulnerability Assessment: 通过跨异构基础架构的优先化补救措施，提供自动化的数据库漏洞检测
- IBM InfoSphere Guardium Data Redaction: 旨在通过检测和删除开放共享文档版本中的数据，预防文档和表单中的敏感数据的无意泄露
- IBM InfoSphere Guardium Data Encryption: 提供企业数据加密，而不牺牲应用程序性能或造成密钥管理复杂性
- IBM InfoSphere Optim™ Data Masking: 能够反识别机密信息，以保护隐私并支持合规性计划
- IBM Security Key Lifecycle Manager: 通过集中化且强化的流程，利用行业标准的密钥管理互操作性协议进行加密密钥生命周期管理。
- IBM InfoSphere Discovery: 该工具通过智能地捕获关系并确定所应用的转换和业务规则，识别并记录现有数据、数据所在位置以及数据在系统间的链接方式

帮助保护应用程序的安全，防御恶意或欺骗性的使用，并抵御各种攻击。

挑战和解决方案要点

IBM应用程序安全产品帮助您：

- 查找并修复移动和Web漏洞：利用静态、动态、运行时和客户端分析，并关联各种结果。
- 构建具有安全设计的应用程序：在整个设计流程中尽早集成安全测试。让安全和开发团队能够有效地通信。
- 控制对应用程序数据的访问：管理和实施细粒度的授权和消息安全策略管理。

产品

旨在保护应用程序的一个完整的解决方案产品组合，包括：

- IBM Security AppScan® Standard: 为IT安全人员、审计人员和渗透测试人员自动化Web应用程序安全测试
- IBM Security AppScan Enterprise: 通过治理、协作和安全智能的企业级应用程序执行安全测试和风险管理
- IBM Security AppScan Source: 通过静态应用程序安全测试，在开发生命周期中识别Web和移动应用程序中的漏洞
- IBM Security Policy Manager: 这些功能可创建应用程序授权和细粒度的访问控制策略，以实现基于身份、事务和服务/资源上下文的分布式策略决策
- IBM WebSphere® DataPower® XML Security Gateway:

一个基于设备的解决方案，可提供实时的Web服务安全和XML威胁保护

基础架构: 网络

抢占式
快速
可扩展

帮助保护整个网络基础架构。

挑战和解决方案要点

IBM网络安全产品帮助您:

- **随时掌握最新的威胁:** 通过IBM X-Force研究成果强力支持的不断演化的威胁保护, 利用帮助防御 "零日" 漏洞的跟踪记录提供网络入侵防御。
- **平衡安全与性能, 无需中断业务关键型应用程序和基础架构:** 使用网络入侵防御功能获得高达20 Gbps以上的检查吞吐量, 从而满足最严苛的服务质量需求——而不会损害安全保护的广度和深度。
- **降低基础架构成本和复杂性:** 通过与其他安全解决方案集成, 整合单点解决方案并降低复杂性。
- **在新威胁出现时迅速保护非网络资产:** 使用IBM Security Network Intrusion Prevention System中可扩展的引擎帮助保护数据、客户端、Web和企业应用程序。

产品

IBM网络基础架构安全产品包括:

- IBM Security Network Protection: 提供核心威胁保护, 以及相关的应用程序可见性和可控功能, 从而帮助减少风险并保护带宽
- IBM Security Network Intrusion Prevention System: 充当网络入侵防御战略的核心, 为针对网络基础架构的广泛攻击提供基于设备的防御
- IBM Security SiteProtector System: 为IBM Security Network Intrusion Prevention解决方案提供集中化的管理, 提供单一的管理控制点, 包括安全策略、分析、警报和报告

基础架构: 端点

评估
修复
实施
报告

帮助保护和管理分布式端点。

挑战和解决方案要点

IBM端点管理和安全产品帮助您:

- **维护所有端点的持续合规性, 无论它们位于何处或使用何种连接:** 部署一个智能代理来监视和报告合规性状态, 并在需要时自动采取更正措施。
- **在异构环境中实现较高的补丁合规性:** 从单一管理控制台和单一管理服务器提供Microsoft Windows、UNIX、Linux和Mac环境, 以及移动设备的补丁修复功能。
- **保护端点, 迅速响应:** 自动识别反常或错误配置的端点, 并在几分钟内识别/修复/隔离遇到事故的端点。
- **简化合规性和风险管理工作:** 通过深入、主动的安全配置审计, 实现自动化和强大的审计和合规性报告。
- **保护虚拟化的端点:** 通过自动保护线上或移动中的虚拟机, 从而获取物理和虚拟服务器环境的单一、集中化的安全视图。

产品

帮助保护分布式端点的IBM产品包括:

- IBM Endpoint Manager: 将端点和安全管理组合到单个解决方案中, 实现物理和虚拟端点的可见性和可控化; 实时、快速修复、保护和报告端点; 以及自动完成跨复杂网络的耗时任务, 从而帮助控制成本, 同时帮助减少风险并支持合规性

- IBM Security Virtual Server Protection for VMware: 通过深度防御、具有虚拟机rootkit检测的动态安全、虚拟基础架构审计，以及通过虚拟机管理程序集成对网络流量的监视，从而保护虚拟基础架构的每一层
- IBM Security Host Protection: 旨在防御对网络资产(包括服务器和桌面)的内部和外部威胁

基础架构: 大型机

合规性管理

利用大型机作为企业安全中心，从而帮助保护任务关键型生产系统和数据。

挑战和解决方案要点

IBM大型机安全产品帮助您:

- **手动验证合规性，仅在出现问题时发出警报**: 通过自动化的合规性监视，获取外部威胁、不当的数据访问或错误配置的实时警报。通过实时拦截IBM Resource Access Control Facility (RACF®)命令，帮助预防特权用户滥用职权。
- **应对识别和分析大型机环境中各种威胁的复杂性**: 自动分析和报告大型机安全事件并检测暴露面。监视入侵者。识别错误配置。
- **保留高技能IT人员来提供手动大型机安全保护**: 使用基于Windows的图形用户界面(GUI)执行RACF管理，从而简化管理工作。

产品

IBM Security zSecure™ Suite旨在提供基础架构大型机安全保护，包括:

- IBM Security zSecure Admin: 使用极少的资源实现有效且高效的RACF管理
- IBM Security zSecure Visual: 通过使用基于Windows的GUI来执行RACF管理，从而帮助减少对稀缺、经过RACF培训的专业知识的需求
- IBM Security zSecure CICS® Toolkit: 来自IBM Customer Information Control System (CICS)环境的大型机管理，释放了本地的RACF资源
- IBM Security zSecure Audit: 自动分析和报告安全事件，并检测安全暴露
- IBM Security zSecure Alert: 实时大型机威胁监视，用于监视入侵者并识别可能危害合规性工作的错误配置
- IBM Security zSecure Command Verifier: 通过预防错误的命令，执行策略以支持对公司和制度策略的合规性
- IBM Security zSecure Manager for RACF z/VM®: 向大型机添加的一个用户友好层，支持对z/VM RACF和Linux on IBM System z® 执行卓越的管理和审计功能

高级安全和威胁研究

世界闻名的IBM X-Force研究和开发团队为IBM的抢占式Internet安全方法提供了基础。这个安全专家小组致力于研究和评估各种漏洞和安全问题，为IBM产品(通过X-Force威胁智能源实时更新)开发评估和应对技术并向公众介绍新兴的Internet威胁和趋势。

IBM X-Force研究和开发有助于保护IBM客户免遭威胁的影响。X-Force漏洞数据库包含超过63,000个已备案的漏洞，并对自1994年以来每次著名的公开漏洞曝光进行了详细分析。每年发布一次的IBM X-Force趋势和风险报告是同类中历史最悠久且最全面的安全研究报告之一。该报告该报告深入分析了安全挑战，包括威胁、操作和开发实践，以及新兴的趋势。

应对当今挑战的解决方案

IBM Security Framework中的集成产品和服务旨在提供安全智能，可帮助您保护当今和未来的企业平台远离已知和未知的威胁。如今，最大的安全趋势和挑战是: 移动安全、云安全、大数据安全和高级威胁。

移动安全

移动设备和平板电脑正快速成为企业及其员工的主要生产力工具，它们提供了随时随地访问信息的灵活性。未受保护的终端设备就像为访问敏感信息打开了大门。组织应保护其设备上的数据——无论数据处于静止状态，还是在不安全的网络和基础架构上移动。IBM帮助组织在一个高度安全的环境中接纳公司和员工所有的移动设备，这个环境中的功能包括:

- **设备安全和管理:** 帮助保护数据和设备
- **安全访问:** 帮助保护企业资源、数据和应用程序
- **应用程序安全:** 帮助确保移动应用程序的设计、开发、测试、交付、使用和管理的安全
- **安全智能:** 给企业提供可见性和一种自适应的移动安全姿态

特色产品:

- IBM Security AppScan Source: 帮助检测移动Web应用程序中的漏洞
- IBM Security Access Manager for Cloud and Mobile: 使用联合SSO、用户身份验证和风险评分将用户访问保护扩展到移动和云环境
- IBM Endpoint Manager for Mobile Devices: 实施设备安全配置和企业管理控制

云安全

组织正在寻找能提供跨多个云基础架构的可见性、可控化、隔离和自动化的云安全解决方案。来自IBM的安全解决方案有助于创建一个云基础架构，能够降低成本并具有如今商业环境所需的动态性。IT部门可通过以下方式减少同管理和云计算有关的风险:

- 跨多个云服务管理身份和单点登录
- 监视对共享数据库的访问
- 在部署到云中的Web应用程序中扫描最新的漏洞
- 帮助保护云用户和工作负载免受复杂的网络攻击
- 通过一种单一、统一的方法监视基于云的和传统的资源
- 提供虚拟机的端点和补丁管理，以实现安全合规性
- 改进多租户环境中云活动的可见性和审计工作

特色产品:

- IBM Security Virtual Server Protection for VMware: 为虚拟基础架构的每一层提供威胁保护
- IBM Tivoli® Federated Identity Manager: 通过单一身份对企业内外的多个云应用程序执行身份验证
- IBM Endpoint Manager: 为分布式云虚拟平台提供高效的安全保护和合规性

大数据安全

激增的企业数据既带来了巨大的管理挑战，又带来了用于获取安全洞察的巨大机会。IBM解决方案从海量的实时和历史数据中提取洞察——在上下文中并超越了以前的可能性。数据是业务的一种新型货币。IBM可通过以下方式帮助保护这种宝贵的资产并巩固企业的安全性:

- 关联来自各个孤岛的海量安全相关数据(例如日志和网络流)，使用集成和智能的安全分析更好地预测和检测业务风险
- 帮助减少来自面临威胁的结构化(数据库)和非结构化(文档)数据的操作风险，帮助防止数据损失和未授权访问

特色产品

- IBM Security QRadar: 面向整个企业的集成、自动化的安全智能和分析
- IBM InfoSphere Guardium: 实时数据库安全和监视，细粒度的数据库审计，自动化的合规性报告

高级威胁

组织在防御高技能且坚决的对手上面临着越来越高的复杂性。这些攻击者可能以关键的IT资产和公共基础架构为目标，使用复杂且现成的技术来获取访问权。

挑战: 没有一个解决方案是万能的。组织必须超越传统的补丁—监视—修复流程，并采用能够彼此协作来识别、分析和响应针对性攻击的持续监视和多层防御。IBM通过以下方式帮助防御高级威胁:

- 通过结合网络安全、全球威胁智能和高级安全分析，从而帮助识别和防御已知以及未知的攻击

特色产品

- IBM Advanced Threat Protection Platform: 包括IBM Security Network Intrusion Prevention System、IBM Security SiteProtector System、IBM Security QRadar Network Anomaly Detection 和 IBM Security X-Force Threat Insight
  - 将X-Force智能注入QRadar，帮助识别与恶意IP地址有关的威胁
  - 帮助防御隐藏在网络流量中基于网络的威胁，并帮助防御攻击者利用网络、主机和应用程序层的漏洞

Gartner将IBM Security分类到领导者象限

企业治理、风险和合规性平台魔力象限，
作者: French Caldwell、John Wheeler，2012年10月4日

用户管理/配备魔力象限，作者: Earl Perkins、
Perry Carpenter，2011年12月22日

静态应用程序安全测试魔力象限，作者: Joseph
Feiman、Neil MacDonald，2010年12月12日

动态应用程序安全测试魔力象限，作者: Joseph
Feiman、Neil MacDonald，2011年12月17日

安全信息和事件管理魔力象限，作者:
Mark Nicolett、Kelly Kavanagh，2012年5月24日

结束语

在大数据世界中，信息是企业的血液，而且对企业数据和IT资产的持久攻击降低了传统IT防御的有效性，所以亟需一种全新的方法。这种方法必须基于3个原则 – 智能、集成和专长 – 并提供基础架构可见性、跨组织链接和必要的优化控制，以便不仅能帮助保护业务关键型数据，还能支持合规性活动。IBM Security Framework提供了一种统一的企业安全方法，能够管理从威胁检测到用户访问、合规性成本削减和配置管理等的关键功能，所有这些功能都以世界闻名的研究和开发成果为基础，有助于减少如今的高级威胁带来的风险。

更多信息

如需进一步了解IBM Security，请联系您的IBM销售代表或IBM业务合作伙伴，或访问：**ibm.com**/security

要加入高级安全研究院，请访问：
www.instituteforadvancedsecurity.com

此外，IBM Global Financing可帮助您以最经济高效的战略性方式获得您的业务所需的软件功能。我们将与信用合格的客户展开合作，定制一个财务解决方案来满足您的业务目标，实现有效的现金管理，以及改善您的总体拥有成本。IBM Global Financing是您进行关键IT投资和向前推进您业务的最智慧选择。有关更多信息，请访问：**ibm.com**/financing

IBM Corporation Software Group Route 100
Somers, NY 10589

在中国印刷
2013年4月

WGB03004-CNZH-00