白皮书

IBM

Tivoli software

通过主机安全管理实现商业价值

目 录

概述

在全球整合市场和极为复杂的动态环境中，信用卡欺诈及数据和保密性违规等犯罪活动令安全性成为重中之重。为了保持竞争优势，公司需要保护自己不受安全威胁，同时关注核心业务活动。IBM Tivoli® Security Management for z/OS® 能够帮助公司将主机用作企业安全中枢来保护环境的安全。这个IBM解决方案能够帮助公司通过以下方式提高投资回报率：

- 简化安全管理，以便提高生产率。
- 通过命令验证来提高管理质量、准确性和策略执行能力。
- 自动审计报告能够提高速度和效率。
- 对所有的金融数据及保密的敏感应用和数据实施一致的循规管理。

迎接现在的安全挑战

公司的系统和数据保密性面临大量安全挑战。在这个全球市场中，为了利用机会并且控制风险，公司必须更加高效地管理运营成本和复杂性，并且交付一致的高质量服务。他们必须要处理好创新、新兴技术及数据量激增带来的内外部安全威胁。此外，公司还必须实施策略并且证明自己满足越来越多规章制度的要求。

摘 要

有效的安全管理必须以业务为上下文并且融入到业务框架中，而不是在问题出现之后才去想办法。

互联网的普遍接入性和匿名接入性令网络犯罪日益猖獗，手段也越来越高明，致使所有的实体都将安全性视为重中之重。技术的进步推动了业务创新，也给网络犯罪提供了温床，导致新的安全威胁层出不穷，加速了各机构对更加先进的安全产品的需求。但是，有效的安全管理必须以业务为上下文并且融入到业务框架中，而不是在问题出现之后才去想办法。

要想迎接现在的安全挑战，公司必须安全地交付服务，同时经济高效地管理威胁和循规活动。公司必须要相信他们的系统使用者，包括员工、客户及业务伙伴，必须要根据组织角色来高效地管理系统访问，必须要保护工资单、在线银行业、贷款申请、零售销量及库存等应用服务的安全性。此外，公司还必须保护整个环境中的数据，无论是静止的数据还是传输中的数据。他们必须扩展并且增强监控解决方案及活动，以便检测威胁和安全漏洞，并且防止保密数据披露和系统故障停机。

降低主机环境中的风险

主机环境中带有强大的硬件、可靠的操作系统、安全的存储系统及可靠的安全组件，素以高弹性、可用性和有效的安全性而著称。鉴于此，许多组织都选择在主机上运行他们的关键应用。此外，这些特征还使主机能够承担起企业安全中枢的重任。

主机安全机制必须能够控制新风险，支持自动审计分析和循规报告，从而大大降低成本和复杂性，同时提供丰厚的ROI。

主机能够促进安全的协作，允许各运营部门使用共享数据集中开展工作，以便公司远离分布式安全环境。公司可利用主机的可扩张性及可扩展性优势将单独的系统整合在一起，以便提高效率、实现并购及收购生成的多个组织之间的协调运营、并且针对所有的计算资源实施标准化系统管理。

企业日益将主机用作管理和数据中枢。经证实，与分布式系统相比，这是降低功耗及许可和场地需求的有效方式。鉴于主机日益被应用到这些全新领域，因此，主机安全机制必须能够控制新风险，支持自动审计分析和循规报告，从而大大降低成本和复杂性，同时提供丰厚的投资回报 (ROI) 。

公司ROI的评估标准是能够直接转变成利润的有形收益。ROI可以降低成本为评估指标，例如，通过增强员工工作能力来提高生产力，借此降低成本；或者直接降低劳动力成本；或者通过可扩展性来降低资本开销等。提高系统可用性、提高服务水平、或者增加员工用在战略计划上面的时间等等，都有助于增强ROI。此外，您也可通过降低安全风险；避免与安全违规相关的罚款、处罚和成本；以及降低与审计和循规工作相关的成本等方式来增强ROI。

本文将介绍公司如何通过IBM Tivoli Security Management for z/OS及IBM System z® 主机提供的高级安全环境来降低成本并且提高ROI。

摘 要

IBM Tivoli Security Management for z/OS是全面的主机安全解决方案，旨在通过安全性管理、用户管理、及面向IBM z/OS RACF的自动审计和循规报告功能来增强并且加速安全管理工作。

IBM提供全面的主机安全性

除传统角色外，主机还日益被企业作为安全或数据中枢广泛部署，因此，公司无论大小，都能通过在System z主机上使用Tivoli Security Management for z/OS获得竞争优势。Tivoli Security Management for z/OS是全面的主机安全解决方案，旨在通过安全性管理、用户管理、及面向 IBM z/OS® Resource Access Control Facility (RACF®) 的自动审计和循规报告功能来增强并且加速安全管理工作。方法如下：

- **简化安全管理** — 提供高效的用户友好层来帮助您实时定义并且赋予用户和组群的访问权限。
- **命令验证和策略执行** — 提供一致的执行策略并且通过拦截和扫描安全命令来帮助您减少安全管理错误。
- **自动的安全审计和报告** — 提供全面的审计功能，能够检测出并且报告主机上的安全事件和信息暴露风险。
- **可与RACF一起运行时提供循规报告** — 使用自动日志功能来收集并且保存事件记录，提供显示板汇总信息并且能够检索事件以备随后调查使用。

通过Tivoli Security Management for z/OS提高ROI

Tivoli Security Management for z/OS的每项主要功能都提供独特的优势来帮助您降低成本、增强ROI，同时管理主机上的风险并且改进服务。

Tivoli Security Management for z/OS提供用户友好层来保住您实时定义并且赋予用户和组群访问权限，从而简化安全管理工作。

通过简化安全管理来实现成本节约

Tivoli Security Management for z/OS提供用户友好层来帮助您实时定义并且赋予用户和组群访问权限，从而简化安全管理工作。这种简单的方法能够最大限度地缩短新用户的调配时间，从而同时提高用户和管理员的生产率。此外，安全管理功能还能为管理员显示所有的用户权限信息并且允许他们交叉引用用户及组群信息，从而帮助管理员决定用户有权接入哪些资源。同样，自动执行命令的功能可以帮助工作台减轻处理密码复位及其他类似问题的工作负担。

管理员可将不同数据库的安全规则有效整合在一起，管理员可以在系统间拷贝或者转移用户、组群、资源、应用或整个数据库。此外，管理员还能使用生产数据库的离线RACF拷贝来编写测试脚本，从而提高系统的可用性并且降低系统对生产数据库的影响。

摘 要

Tivoli Security Management for z/OS能够降低与策略和安全管理任务相关的管理成本，从而帮助您实现巨大的成本节约。此外，该产品还能通过缩短用户等待时间来提高生产率。

公司还能通过Tivoli Security Management for z/OS的安全管理功能从其他多个方面实现成本节约。例如，用户可实时查看活动RACF数据库中的数据，以便了解变更产生的影响，无需等到未装载的RACF数据库更新完成之后。管理员还能将开展相同工作的用户进行比较，以便决定他们是否接入了相同资源，从而确保只允许用户根据工作需要访问适当资源。

此外，管理员还能选择任何指定数据集并且查看访问这些数据的用户清单，从而快速发现错误，以防它们真正威胁到安全性和循规性。简单的安全管理功能也能支持高效的RACF数据库清洗操作，从而帮助您提高数据完整性，借此增强数据的价值。

一所大学的IT部门通过使用Tivoli Security Management for z/OS的简单安全管理功能不仅实现了上述优势，而且还在其他领域有所斩获。这个IT部门由两名系统程序员和一个帮助台组成。帮助台的任务是密码重置，而系统程序员的任务则是在主机中创建全新的用户ID并且定义用户访问权限。系统程序员希望利用适当的解决方案来简化学生用户ID的创建与维护流程。

通过实施Tivoli Security Management for z/OS，系统程序员在RACF的基础上又添加了一个用户友好层来简化安全管理流程，借此帮助IT部门节省劳动力。他们可使用这个用户友好层为用户和用户群定义访问角色并且赋予他们访问权限、设置并且重置用户ID和密码、显示用户ID或用户群的所有权限信息或交叉引用这些信息。IT部门工作压力减轻后，系统管理员可将更多时间用在开展高价值的工作上。

Tivoli Security Management for z/OS的Command Verifier功能提供策略执行功能，能够保护您的系统远离内外部安全违规风险。

通过命令验证和策略执行功能来减少代价高昂的错误及安全风险

Tivoli Security Management for z/OS的Command Verifier功能能够执行安全策略，通过拦截和扫描安全命令来发现存在风险的命令、生成警报、创建审计记录、并且可能会在执行命令之前选择拒绝或修改命令。Command Verifier能够执行多个安全策略，如命名惯例、严格的安全违规监控、安装时的标准访问权限、以及控制安全管理员的特权和命令等。

Command Verifier可以限制管理员的权限、防止他们犯错误、并且能够检测出可能存在的管理特权滥用事件。因此，能够保护您的系统远离有意或无意的安全违规行为。Command Verifier允许管理员快速检测出策略违规事件，从而及时扼制住可能造成安全信息暴露或权利滥用的问题。由于Command Verifier是自动执行的功能，因此能够自动执行策略、减少错误并且最大限度地减少重复工作，从而帮助您大大降低循规管理成本。此外，Command Verifier还提供安全工具定制功能，以便满足您的特定需求，无需您冒险安装出口程序。

摘 要

一家政府机构通过使用Tivoli Security Management for z/OS的Command Verifier功能控制了可能造成数百万美元罚款的风险，从而提高了ROI。

一家政府机构通过使用Tivoli Security Management for z/OS的Command Verifier功能提高了ROI。这家机构希望主机安全解决方案能够帮助他们满足安全政策及审计制度的要求。通过实施Tivoli Security Management for z/OS，这家政府机构不仅能够提取活动RACF数据库的快照，而且还能通过卸载文件来分析系统安全状态。此外，他们还能报告存在问题的系统选项及危险的特权用户设置，同时自动开展System Management Facility (SMF) 分析工作，检测库的变化，并且跟踪安全设置的变化。

实施Tivoli Security Management for z/OS之前，这家政府机构的特权用户由于无意犯下配置错误和粗心下达安全命令给他们带来了数百万美元的损失。此外，拥有访问权限的恶意用户更是令事态变得雪上加霜。Tivoli Security Management for z/OS能够控制这些风险，不仅令这家政府机构感到放心，更是帮助他们实现了丰厚的投资回报。

Tivoli Security Management for z/OS提供全面的审计功能，能够检测出并且报告主机安全事件和信息暴露风险，从而建立全面的审计跟踪机制。

通过自动执行安全审计和报告任务来降低管理成本

Tivoli Security Management for z/OS提供全面的审计功能，能够检测出并且报告主机安全事件和信息暴露风险。Tivoli Security Management for z/OS能够通过分析SMF日志文件来创建包括RACF、IBM DB2® 和UNIX® 的全面的审计日志（见图1），从而允许管理员简化并且自动化主机事件处理流程。

可定制的报告能够区分安全问题的优先级，从而允许管理员首先解决最重要的问题。管理员可选择只有在发生特定事件或者出现安全违规时，才会每天接收一次报告。此外，该产品的审计组件能够自动将主机安全事件信息发送给循规管理组件，以便生成适当的报告。

自动策略管理和入侵管理功能能够大大减轻管理负担。自动审计分析功能可以缩短检测时间，自动报告和报警功能允许您快速响应安全事件，以便抵御威胁并且缩短故障停机时间。由于该产品还能自动修复许多问题，因此允许IT管理员将更多的时间用在开展更重要的工作上。此外，与审计需求相一致的自动化流程还能帮助您缩短审计准备时间。

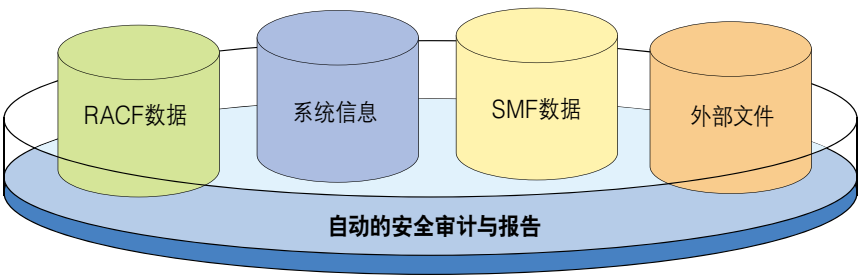

图1: Tivoli Security Management for z/OS为RACF、DB2和UNIX提供自动安全审计、报告和报警支持。

摘 要

一家大型欧洲金融服务机构通过使用Tivoli Security Management for z/OS的自动策略管理和入侵管理功能提高了ROI。该公司希望通过适当的解决方案来替换现有的主机安全软件，以便简化审计、在线报警和报告流程，同时降低主机平台的总体拥有成本。部署Tivoli Security Management for z/OS伊始，他们便能轻松发现并且修复审计问题，从而受益匪浅。该系统能够为审计问题自动分配优先级，以便公司做出有效的安全规划并且为修复工作分配优先级。使用该产品提供的报告语言，公司生成了周管理报告以供高级管理人员和内部审计人员查看，以便他们能够跟踪全部的审计问题，并且逐周减少这些审计问题的数量。

通过实施Tivoli Security Management for z/OS，尽管这家金融服务机规模很大，但却能够仅仅通过三名专业人员来管理多个RACF环境。通过自动安全审计和报告功能，这个解决方案不仅帮助公司解决了安全管理问题，而且还降低了与管理员工信息访问相关的成本，缩短了相关时间。

一家著名的欧洲保险公司通过实施Tivoli Security Management for z/OS 大大降低了管理成本。

一家著名的欧洲保险公司指出，通过实施Tivoli Security Management for z/OS，他们取得了以下的管理和审计优势：

- 持续不断的自动审计与纠错控制每年可帮助公司节省1个月的（数据）清洗工作时间。
- 使用产品的报告语言而不是其他编程语言来创建定制报告，从而每年能够节省1-2个月的工作时间，包括降低CPU需求。
- 为管理任务生成大批RACF命令，每年也能节省2个月的工作时间。
- 面向业务部门的自助服务及自动报告功能每年可以节省1个月的报告制作时间。

Tivoli Security Management for z/OS提供显示板来显示整个环境中的活动情况。

一致的循规报告能够缩短审计时间并且降低成本

为了帮助您有效管理安全循规工作，Tivoli Security Management for z/OS提供显示板来显示整个环境中的活动情况。Tivoli Security Management for z/OS的循规工具能够使用自动日志功能从几乎任何平台上收集、保存、调查和检索日志，从而允许您将主机日志集成到企业报告中（见图 2）。

若与Tivoli Compliance Insight Manager配合使用，Tivoli Security Management for z/OS还能提供高级报告引擎来创建报告，以便记录您对“健康保险可移植性与责任法案”（HIPAA）、“支付卡行业（PCI）数据安全标准”、“萨班斯·奥克斯利法案”（SOX）、国际标准组织（ISO）各项法案、Basel II及其他规章制度或标准的遵从情况。这项经济高效的循规监控与报告功能构建了一条安全管理环路（见图 3），允许您针对系统中的安全暴露事件采取适当的纠正措施。

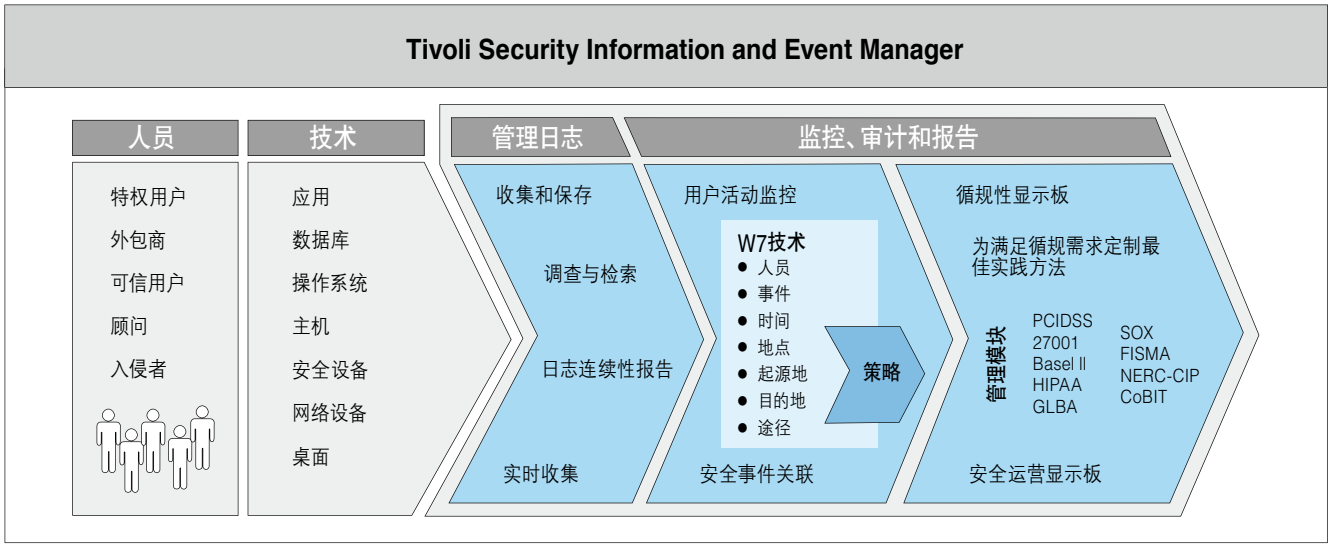

图2: Tivoli Security Management for z/OS, 结合Tivoli Compliance Insight Manager，提供显示板来帮助您跟踪整个环境中的循规情况。

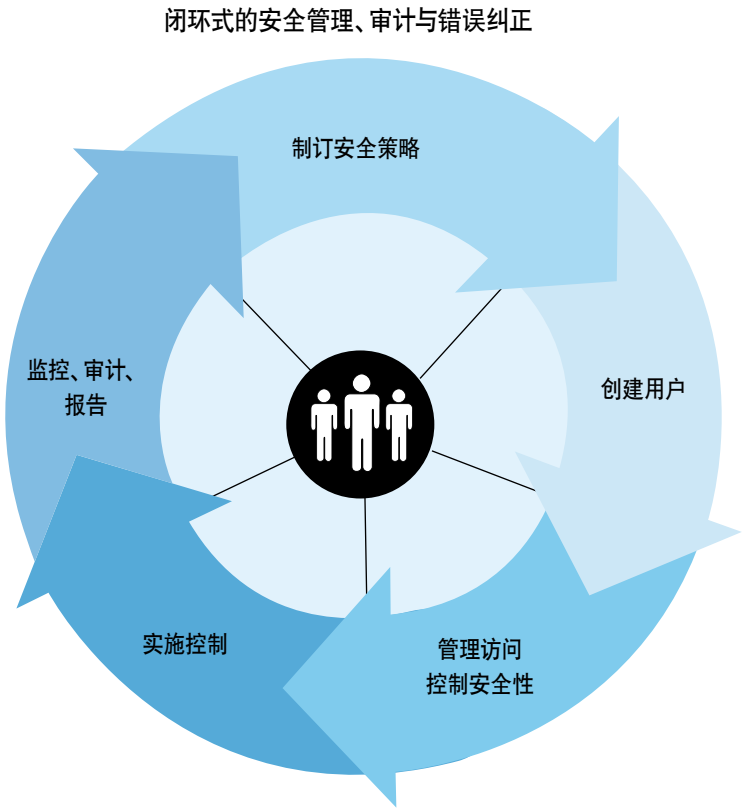

图3: Tivoli Security Management for z/OS提供全面的循规功能，构建了一条封闭的安全环路。

Tivoli Security Management for z/OS的自动循规报告功能能够减轻管理和审计负担并且缩短提供循规证据所需的时间，从而节省大量成本。自动日志管理功能则允许您轻松开展普遍

摘 要

英国的Aviva公司成功避免了与手动制作循规报告相关的大量劳动力成本，并且减少了与循规活动相关的错误。

的信息收集、保存、检索和调查工作。集成分析功能能够帮助您分析用户行为，降低因内外部威胁而遭受损失的风险。

Aviva通过使用这些自动循规报告功能而提高了ROI。作为欧洲著名的寿险和养老金产品运营商，Aviva需要在其IT环境中实施具有预防能力、检测能力和纠错控制能力的产品，借此来提高循规能力。公司实施了Tivoli安全解决方案来满足异构主机环境的需求并且提高了循规能力，以便满足越来越严格的安全政策、法规及规章制度的要求。

这个解决方案提供健壮的审计和循规报告功能，帮助公司提高了循规能力、增强了循规活动的效率、并且减少了错误。此外，Aviva还成功避免了与手动制作循规报告相关的大量劳动力成本以及因为错误而导致违规的成本。

主机是企业安全中枢

通过Tivoli Security Management for z/OS，IBM允许您将主机用作企业安全中枢发挥作用。此外，通过提供更多的组件来满足用户调配、联合身份管理、访问理、加密密钥管理、审计报告和循规管理需求，Tivoli Security Management for z/OS能够为您的整个环境提供卓越的安全保护（见图 4）。

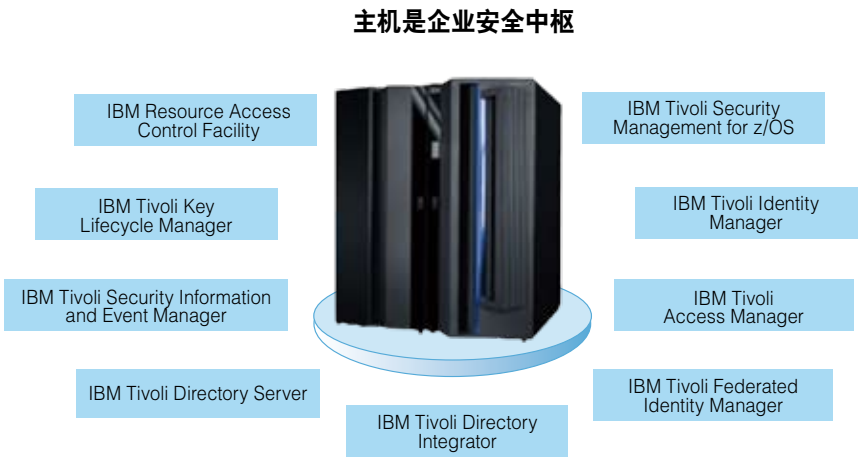

图4：Tivoli Security Management for z/OS与其他的主机安全产品配合工作，允许您将主机用作企业安全中枢。

IBM 将安全功能与服务请求管理功能集成在一起，通过自助服务密码管理功能来减轻服务台的工作负担，同时仍支持服务台开展必要的事故跟踪工作。

摘 要

Tivoli Security Management for z/OS提供闭环式的集成安全信息和事件管理环境，能够管理身份和访问权限。

Tivoli Security Management for z/OS还提供闭环式的集成安全信息与事件管理功能，能够对身份和访问进行管理。因此，您可以在整个信息生命周期中利用身份管理功能。该产品还能持续监控用户、用户权限以及用户对这些权限的使用情况，以便快速诊断并且立刻修复安全信息暴露问题。

您可通过Tivoli Security Management for z/OS来保护和审计关键业务服务，以便利用这个高弹性的可信平台。您还能：

- 通过利用企业中最安全的平台来改进服务。
- 通过数据中心整合、嵌入最佳业务实践及自动执行循规任务来降低成本。
- 更好地满足数据披露和保密制度的要求，并且做好审计准备工作，从而管理风险。
- 避免与安全违规相关的、不断增加的巨额成本。

Tivoli Security Management for z/OS的应用

爱尔兰联合银行通过Tivoli安全产品替换了原来的主机安全软件，使公司能够提前扼制住安全威胁并且降低了循规成本。

爱尔兰联合银行 (AIB) 希望提高零售客户服务的灵活性和经济高效性。AIB请求IBM帮助他们更换主机安全系统。银行需要部署全面的安全解决方案来帮助他们执行安全策略并且自动满足多个环境的管理和审计需求。

AIB通过IBM RACF和Tivoli安全产品替换了原来的主机安全软件，以便提前预知安全威胁并且降低循规成本。AIB现已能够主动审计安全配置，以便检测出并且报告安全风险和其他担忧。此外，IBM产品还能实时监控AIB环境，以便发现配置错误、安全暴露风险和入侵者，允许管理员立刻采取纠正错误。AIB现在还能接入可定制的全面的报告，从而减轻审计负担，同时满足“萨班斯·奥克斯利法案”等安全和审计制度的要求。他们能够自动跟踪z/OS和RACF安全级别的变化，从而决定系统资源是否存在风险。

用户友好的界面、交互式命令生成、自动化进程及在线帮助等功能，均可帮助AIB的安全管理员快速获得所需的z/OS和RACF安全技能。这个新系统已经帮助AIB解决了安全问题，使管理员能够减轻安全管理工作负担，集中精力开展高质量的安全管理活动。

摘 要

IBM提供商业价值评估服务，以便您的公司能够快速评估将Tivoli Security Management for z/OS作为企业安全解决方案进行部署的商业价值。

为Tivoli Security Management for z/OS构建商业案例

IBM 提供商业价值评估服务，以便您的公司能够快速评估将Tivoli Security Management for z/OS作为企业安全解决方案进行部署的商业价值。通过这项重要服务，IBM可以帮助您决定如何怎样的战略来增强主机环境的安全性以及如何通过实施全新解决方案来实现预期ROI。

更多信息

如想详细了解Tivoli Security Management for z/OS或者请求IBM提供商业价值评估，请与当地的IBM业务代表或IBM业务伙伴联系，或者访问：**ibm.com**/tivoli/solutions/security。

可回收，请回收再利用

TIW14038-USEN-00