IBM

Tivoli software

利用IBM System z和IBM Tivoli安全解决方案，增强您的企业安全

要 点

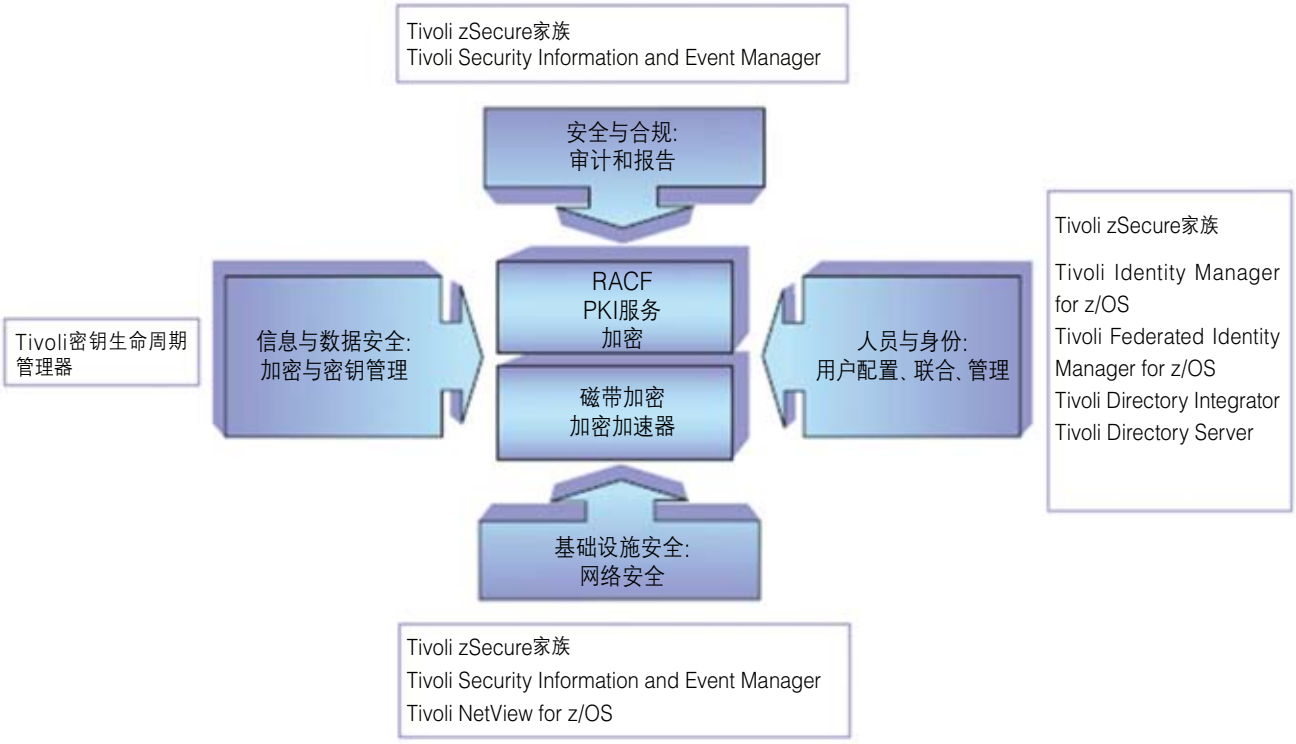
- *增强对安全和合规漏洞的整体了解，关注您的关键优先任务和问题*
- *简化安全管理和身份管理，并自动响应威胁和合规风险，帮您预防欺诈*
- *利用IBM System z®作为企业安全中枢，帮助降低数据保护成本，最大限度降低风险*

在当前联网的世界中，随着黑客和内部人员不断地渗透到网络中并威胁系统和数据安全，企业面临着持续的威胁。信息必须以安全的方式得到保护，将企业置于符合法规和法律要求的框架内。加密静态数据并不足以满足要求，因为信息在网络中传送，而且可能在多个地点面临着潜在风险。企业必须防止外部和内部人员威胁其业务运作和信息。

许多企业利用能够应对不同威胁的大量终端产品保障安全。这种方法可导致安全漏洞，包括巨大的和细小的漏洞，而这些漏洞可能被恶意用户利用，在伤害最严重的方面影响企业的运作——财务和品牌资产。

关于数千客户记录被盗的报道对公司的影响速度比任何情况都要快。

安全点解决方案仅提供了暂时的权宜之计。企业需要通过使用自动化解决方案持续地了解并控制安全环境，因为威胁永远



ITCAM for Transactions自动生成交易基础设施的拓扑，用于实现端到端的交易追踪。

不会停止。例如，建立身份控制规则，自动监控有权限用户的活动非常重要。IBM Tivoli®安全和合规管理产品可为企业提供这些以及其它方面的能力，以实现对企业安全的持续警戒。

IBM Tivoli安全管理产品旨在补充System z软硬件的优势，并且共同帮助企业将System z用作企业安全中枢。

System z服务管理中心简介

System z的IBM Tivoli服务管理中心战略使企业能够更轻松地将System z用作集中、高效管理业务和IT服务的中枢。IBM System z主机凭借其整体的、包含丰富安全功能的设计，始终被作为企业安全中枢的首选。主机提供了精细的接入控制和网络安全特性，可减少威胁，而内置的加密解决方案可帮助企业更好地防止数据遭窃或受到安全威胁。

现在，利用IBM服务管理，企业可以进一步扩展System z投资所建立的管理中枢的优势，以建立一个以业务为驱动的IT组织，从System z中利用跨复杂应用环境的简化视图和控制措施来提供管理服务。System z服务管理中心战略结合了流程管理、服务管理和操作管理的最佳实践和服务，使企业能够更好地了解企业中的异构系统和应用。

Tivoli Service Management Center for System z的组件可协同运行，帮助企业满足大量的IT管理需求。作为本战略的一部分，Tivoli安全解决方案有助于建立一个安全框架，可为利用高可靠性和高可用性的

System z主机作为企业安全中枢而提供必要的洞察力和控制力。通过在本战略的运作范围内采用这些安全解决方案，您可以利用端到端的安全和合规政策控制您的IT基础设施，并帮助保证您的企业受到全面保护。

安全与合规

高效的安全取决于对信息资产和事件的洞察力。过去，信息安全主管可以使用安全软件提供的标准工具每天有效地监控安全事件。当前环境由于采用一套异构系统而使复杂性提高，这需要采用整合的解决方案来统一、有效且不间断地进行这项工作。

IBM Tivoli zSecure套件采用同时针对CA ACF2的实时监控能力，为IBM Resource Access Control Facility (RACF®)系统和其它解决方案提供了深入的审计和实时监控能力，例如CA ACF2 (包括安全数据库支持)和CA Top Secret (在系统管理设施层面。zSecure产品家族与IBM Tivoli Security Information and Event Manager可帮助支持企业的审计响应和报告要求。

Tivoli Security Information and Event Manager集成了IBM Tivoli Compliance Insight Manager和IBM Tivoli Security Operations Manager的能力。

主机事件和告警数据被传送到Tivoli Security Information and Event Manager，以提供涵盖整个企业的洞察力。该软件还集成了网络事件监控能力，使您能够隔离可能违犯规则的网络漏洞。

Tivoli Compliance Insight Manager将RACF、IBM DB2®、IBM z/OS®、CA ACF2和CA Top Secret安全信息收集到整个企业的合规仪表板中，以统一的格式用于报告目的。这允许用户查看其企业安全中枢的状态，调查安全事件，并且报告有权限用户的活动。此外，它还包括现成的或定制的报告，以满足特定法规的要求，包括HIPAA、GLBA、SOX、PCI、Basel II、ISO17799和SAS70、Tivoli Compliance Insight Manager允许您获得关于安全的整体视图——不仅是IBM系统，而且也包括其它企业资源。

Tivoli Security Operations Manager提供了关于主机威胁和事故的全面视图。

该解决方案实时收集并分析网络中安全设备的信息。通过先进的关联能力，它能够识别安全事故，确定其优先级，并允许企业自动应对这些事故。

人员与身份

有效控制接入网络、系统、应用和数据的用户身份和进程是最基本的信息安全要求。无论威胁来自内部或外部，分散地管理用户身份并监控潜在身份安全威胁是实现安全保护和合规的基本要素。

Tivoli zSecure套件提供了RACF安全和监控的管理与政策执行。这个安全套件为主机环境增加了一个用户友好的接口层，在提供卓越的管理能力的同时，还提供了全面的审计、告警和监控工具。Tivoli zSecure套件通过将您的信息安全人员从普通的例行任务中解脱出来，使他们集中精力开展重要的安全管理活动，从而以更低的总体成本提供了全面的主机安全。

zSecure套件通过与其它Tivoli和IBM软件产品集成开展其价值，为企业提供了更全面的整合的安全、身份和接入管理能力。这些能力可帮助企业整合安全控制措施，提高安全操作与流程的效率，减少与孤立安全功能相关的漏洞，并且降低安全保障的总体成本。

IBM Tivoli Identity Manager for z/OS®利用IBM System z主机的可靠性、可用性、扩展性和性能，为对z/OS上和来自z/OS的用户进行身份管理提供了一个中枢。

Tivoli Identity Manager可向登记表中配置并更新企业内的用户账户，包括LDAP目录、UNIX®系统。Microsoft® Windows®和z/OS的特定登记表，例如RACF、CA Top Secret,和CA ACF2。

IBM Tivoli Federated Identity Manager for z/OS简化了应用集成，并增强了对于谁访问应用中的数据的了解。它提供了一个集中的身份采集服务，用于验证分布式环境的身份信息，并提供了RACF PassTickets，允许进行独特用户识别，并允许接入主机应用。

Federated Identity Manager运行于z/OS上，可作为一项集中服务，处理企业SOA基础设施中的安全证书转换请求。

IBM Tivoli Directory Server提供了高可用性、高扩展能力、高性能、基于LDAP并支持多种平台的目录，为全面且灵活的身份管理提供了动态、可扩展的模式。IBM Tivoli Directory Integrator提供了实时的、事件驱动的数据同步，可为身份和其它数据建立一个权威数据源，有助于实现数据完整性，并降低手动操作成本和维护风险。Tivoli Directory offerings作为IBM身份和接入管理产品的基础，为实现整合的安全架构提供了紧密地目录集成。

基础设施安全

安全漏洞有时可以预测，因为恶意破坏者通常尝试通过多种机制穿透客户的环境，例如利用网络弱点和尝试多种形式的攻击。

您拥有能够防护网络，帮助检测漏洞和识别恶意活动来源的系统至关重要。

Tivoli Security Information and Event Manager允许您管理、处理、关联并分析大量的安全和网络事件。它提供了来自安全操作中心和网络运行中心的相关安全告警的现成链接，使管理员能更好地了解安全事故对业务的影响。Tivoli zSecure软件增强了企业对主机的内部政策、外部法规、业务应用、中间件、数据、系统和网络的洞察力。

Tivoli NetView for z/OS与System z Communication Server的入侵检测服务器(IDS)配合，提供了对入侵行为的自动响应。这些响应包括通过控制台或电子邮件向操作员发送简单的通知，通过执行命令而采取措施，例如自动关闭受攻击的端口，防止试图发起攻击的人进入RACF或ACF2。

信息和数据安全

保护数据的隐私并不仅仅是一个良好的业务实践——在很多情况下，它是一项法律要求。企业需要这样的解决方案：能帮助保护企业内的数据和信息资产的安全，并帮助确保一致且持续的保护，从而帮助降低风险。加密密钥的管理是良好的安全实践和法规遵从的前提。

对于必须管理企业内用于供应商、应用和设备的密钥的企业，密钥的管理和分发已被证明是一项棘手的任务。IBM Tivoli Key Lifecycle Manager帮助完成这个至关重要的任务，通过增强信息完整性而帮助用户管理信息风险，促进加密密钥保留政策的实施，并且简化数据恢复。

将System z用作企业的安全中枢

在针对System z的Tivoli服务管理中心模式内，Tivoli安全解决方案提供了：

- 来自RACF、应用、数据和系统的安全相关事件与威胁的自动检测、收集、分析和告警。
- 全面的审计和合规管理与报告能力。
- 汇总IT基础设施内的安全事件和合规状态数据。
- 简化且自动化的安全操作管理能力。
- 复杂环境的身份和接入管理能力。
- 利用经过改进的加密密钥管理和接入报告而增强数据保护能力。

其好处包括提高IT效率并降低合规风险和安全管理的成本，同时利用System z作为企业的安全中枢。

更多信息

欲了解关于针对System z的IBM Tivoli服务管理中心和IBM Tivoli安全产品的更多信息，请联系您的IBM销售代表或IBM业务伙伴，或访问：**ibm.com**/tivoli/features/zsmc/和ibm.com/tivoli/solutions/security

关于IBM Tivoli软件

Tivoli软件为企业提供了一个服务管理平台，用于通过实现洞察力、控制力和自动化而提供卓越的服务——洞察力是指查看并了解业务活动；控制力是指有效地管理业务，帮助最大限度降低风险，并保护品牌；而自动化是指帮助优化业务，降低运作成本，并更快地推出新服务。与以IT为中心的服务管理不同，Tivoli软件为管理、集成和协调业务与技术要求提供了一个通用的基础。Tivoli软件的设计旨在快速满足企业最急迫的服务管理需求，帮助主动应对不断变化的业务需求。Tivoli软件系列以世界一流的IBM服务、IBM支持和积极的IBM业务伙伴网络为依托。Tivoli客户和业务伙伴也可以通过参与独立运作的全球IBM Tivoli用户组而互相共享最佳实践——请访问：www.tivoli-ug.org

印制于中国
2010年7月

TIS14030-USEN-00