IBM软件
信息安全解决方案

IBM Security

系列产品宣传手册

IBM SECURITY

CONTENTS

概 述

1

IT安全已成为一个热点问题

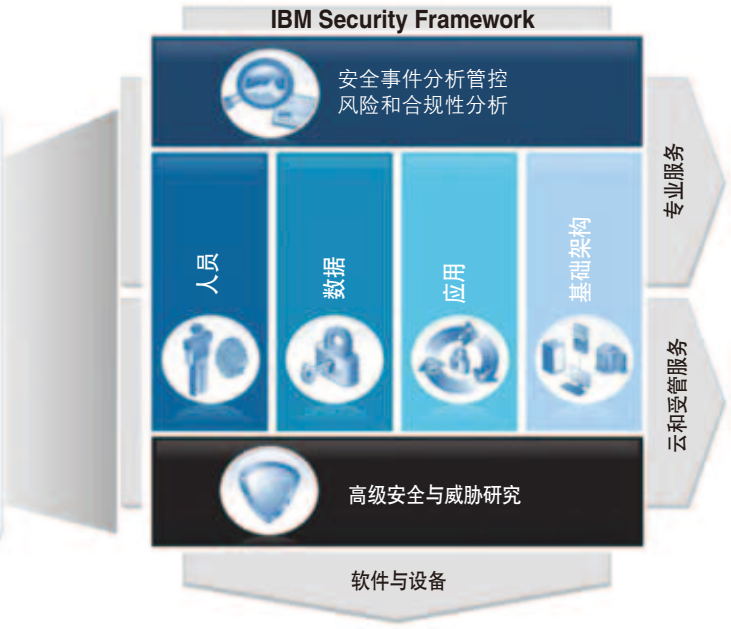
IT安全风暴来袭。黑客越来越高明，您的数据也随时随地被访问，而且常常存在于云中。企业控制了越来越少的访问点，同时数字数据也在飞速增长，员工和系统的合规性要求也在不断增加。

这些趋势都意味着企业IT安全不再是一个仅需事后考虑的问题，也不是划定好安全界限就可以得到解决。相反，安全智能防护、随时检测和解决系统漏洞必须被提上日程，成为组织IT结构的一部分。IT安全现已成为组织日常业务运营不可或缺的部分。

全新的IBM部门: IBM Security Systems

IBM Security Systems

- 实现安全技术架构端到端的覆盖
- 有超过6000名的安全顾问和技术服务专家
- 有备受赞誉的X-Force® 研究机构
- 业界最大的安全事件库



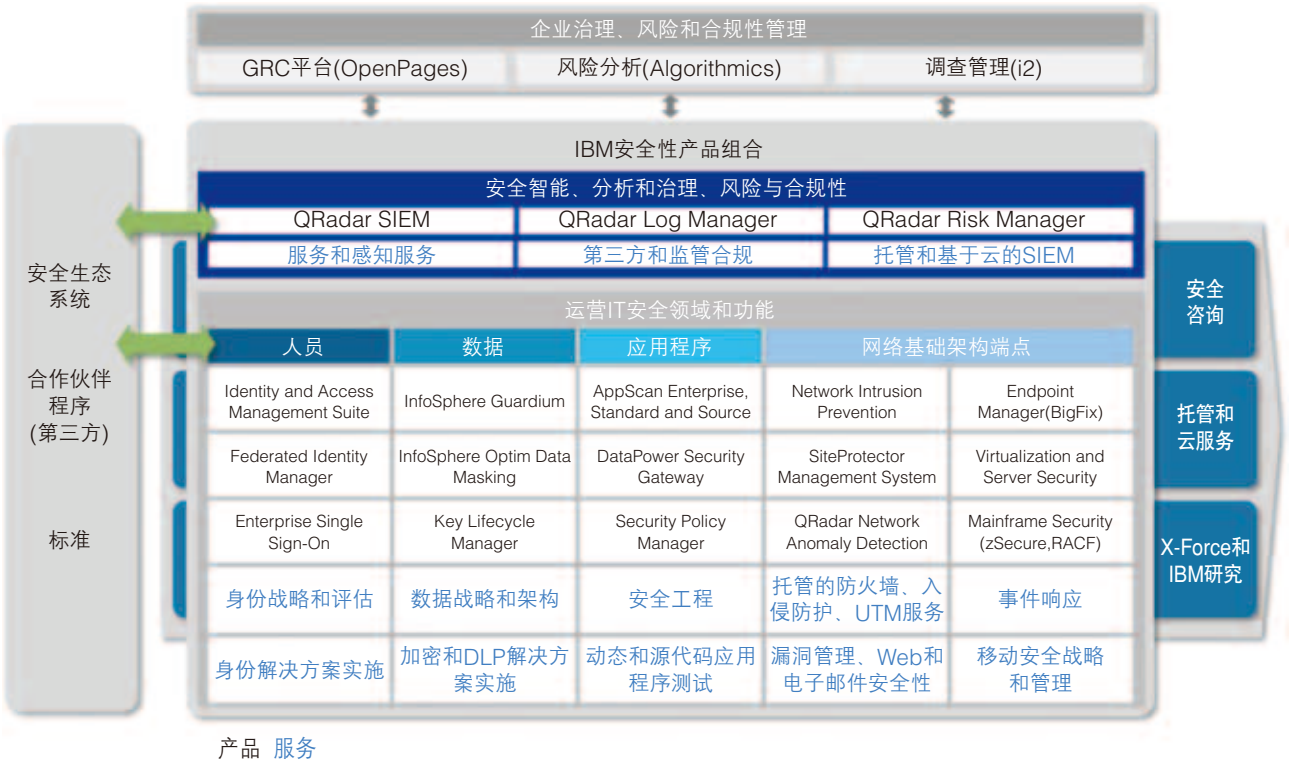
”IBM安全解决方案”通过一个完整的安全框架帮助您实现IT安全管理，这个框架包括硬件和软件，还有服务专家会针对您的独特需求定制整合安全解决方案，帮助您降低总体拥有成本。

IBM拥有一个全球最完善的企业安全研究、开发和交付组织，有6,000多位研究者、开发人员和主题专家参与安全研究活动。这些强大的安全专业综合知识来自获奖的X-Force研究和开发团队——他们具有业内最大的漏洞数据库，有9个安全运营中心、9个IBM研究中心、14个软件安全开发实验室，还拥有IBM Institute for Advanced Security，在美国、欧洲和亚太地区都有其分部。

目前，IBM每天要监控130多个国家/地区安全中心的130多亿个安全事件。IBM拥有大量顾问和专家帮助任何组织通过安全智能实现优化、整合的安全控制。

因此，不管您的风险是来自高级威胁、移动访问，还是云架构、合规性问题；或者您正在力求通过分析大数据获得安全洞察，那么，来自IBM安全解决方案的工具和专家都可以帮助您实现这一切。

智能: 产品和服务的全面组合



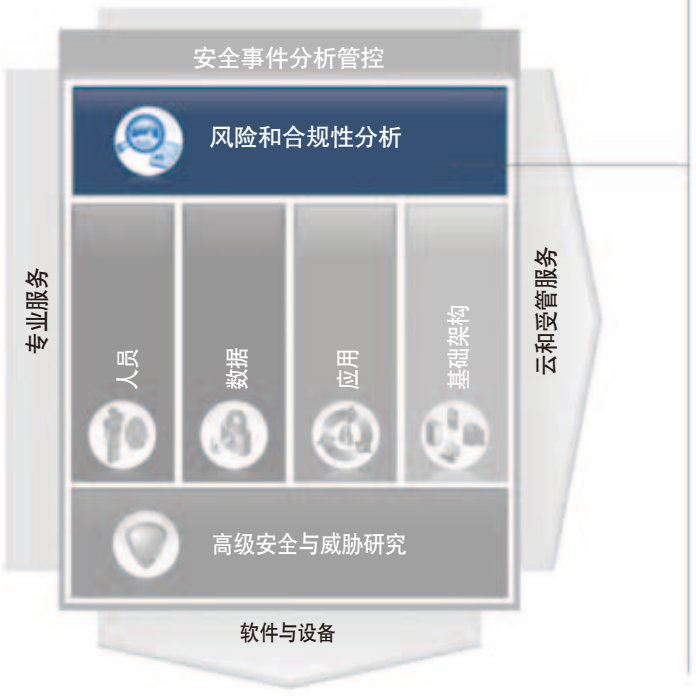
安全智能

2

安全智能和大数据

研究领域

利用额外的上下文、自动化和集成帮助客户优化安全性



产品组合概述

QRadar SIEM

- 日志、流、漏洞和身份关联
- 成熟的资产分析
- 违规管理和工作流

QRadar Risk Manager

- 预测威胁建模和仿真
- 可扩展的配置监测和审计
- 先进的威胁和影响分析

QRadar Log Manager

- 交钥匙式日志管理和报告
- SME 到企业
- 可升级至企业 SIEM

Network Activity Collectors (QFlow / VFlow)

- 网络分析、行为和异常检测
- 完全集成 SIEM

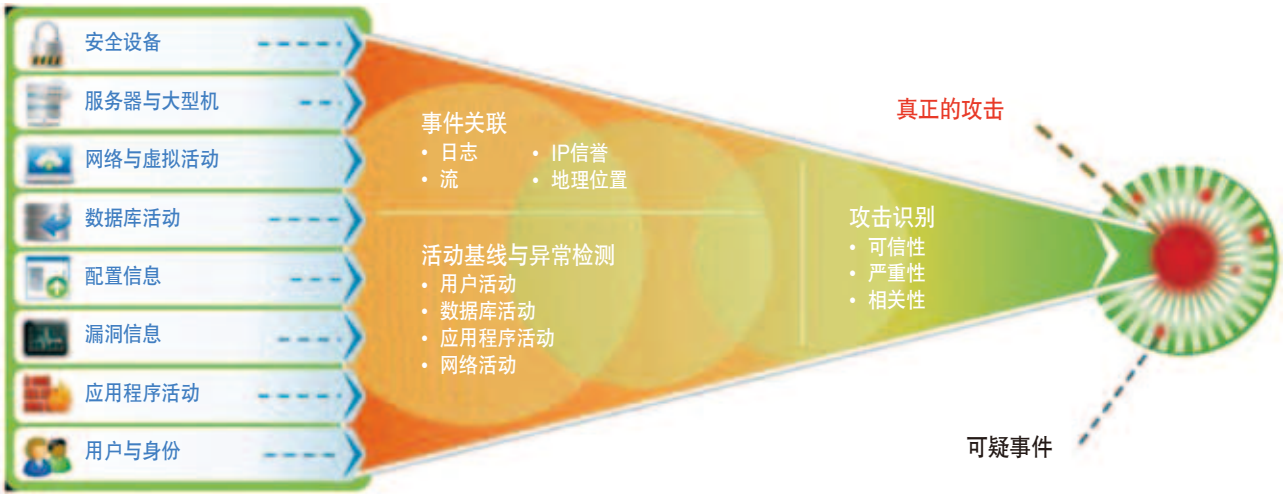
当组织暴露时，无论数量还是种类，都比以往任何时候面临更多的威胁及合规风险。IBM安全智能解决方案在您的组织中利用与安全相关的信息，采用先进的智能，帮助您更快地检测威胁，更有效地确定风险的优先次序，同时自动化合规活动。

IBM QRadar Security Intelligence Platform在分布式和可扩展的安全信息存储库中应用实时关联和异常检测。大数据分析可以实现更准确的安全监控和更好的可视性，并且可以打包后供小型组织与大型企业使用。通过卓越的易用性、灵活性和预包装的功能，IBM解决方案帮助您更快地实现价值，并伴随业务的变化来发展您的部署。

各种行业中的客户使用IBM QRadar Security Intelligence Platform来实现:

- 检测高级的威胁
- 解决监管合规要求
- 检测内部威胁和欺诈行为
- 预测对企业的风险
- 整合数据竖井

安全智能解决方案提供了SIEM(安全信息和事件管理)、日志管理、配置和漏洞管理、行为分析和异常检测功能——通过一个集成的灵活平台提供这一切。了解更多关于中小型企业、大型企业、非营利组织和政府机构如何利用IBM解决方案改善其安全状况，自动化合规，并降低其总拥有成本。



Security Intelligence关联一组不同的安全相关数据，以获得切实可行的洞察

2.1 QRadar SIEM

IBM® Security QRadar® SIEM将来自分布在整个网络中的数千个设备端点和应用程序的日志源事件数据整合在一起。该软件对原始数据执行即时的规范化和关联活动，从误报中甄别真正的威胁。作为一种新的选择，该软件纳入了IBM Security X-Force® Threat Intelligence，提供了一个潜在的恶意IP地址列表，包括恶意软件的主机、垃圾邮件的来源和其他威胁。IBM Security QRadar SIEM也可以关联系统漏洞与事件及网络数据，帮助确定安全事件的优先级。

IBM Security QRadar SIEM:

- 提供近实时的可见性，实现威胁检测并确定优先级，在整个IT基础架构中提供监控。
  - » 帮助检测可能会淹没在数百万个事件中的应用程序的不当使用、内部欺诈，以及先进的较低、较慢的威胁。
  - » 从多个资源收集日志和事件，包括安全设备、操作系统、应用程序、数据库，以及身份和访问管理产品。
  - » 从交换机和路由器收集网络流数据，包括第7层(应用层)的数据。
  - » 从身份和访问管理产品及Dynamic Host Configuration Protocol (DHCP)等基础架构服务获取信息；并从网络和应用程序漏洞扫描器接收漏洞信息。
- 减少警报并确定警报的优先级，根据可疑事件的可操作列表进行重点调查。
  - » 执行即时事件规范化并与其他数据相关联，实现威胁检测及合规性的报告和审计。
  - » 将数十亿个事件和流程减少为少量几个可操作的违规，并根据对业务的影响确定其优先级。
  - » 执行活动基线确定和异常检测，以识别与应用程序、主机、用户和网络区域有关的行为变更。
  - » 选择性地使用IBM Security X-Force Threat Intelligence，以识别与可疑IP地址相关的活动，如涉嫌托管恶意软件的活动。
- 实现更有效的威胁管理，同时形成详细的数据访问和用户活动报告。
  - » 跟踪重要事件和威胁，提供对所有支持数据和上下文的链接，以方便调查。
  - » 以近实时流式传输模式或在历史的基础上执行事件和流数据搜索，以增强调查。
  - » 支持添加IBM Security QRadarQFlow和IBM Security QRadarVFlow Collector设备，通过第7层的网络流量采集，获得对应用程序(如企业资源管理)、数据库、协作产品和社交媒体的深入洞察和可见性。
  - » 帮助检测应用程序或基于云的服务的非工作时间或异常使用，或者是不符合历史使用模式的网络活动模式。
  - » 在大型的、地理上分散的环境中执行联合搜索。
- 支持更容易、更快的安装，并包括节省时间的工具和特性。
  - » 自动发现大多数日志源设备，并监控网络流量，以找出主机及服务器(跟踪应用程序、协议、服务及其使用的端口)并进行分类，以节省大量时间。
  - » 包括一个集中式用户界面，通过函数和全局视图来访问近实时分析、事故管理和报告，从而提供基于角色的访问。
  - » 将短时间内发生的网络流量记录分组为单个条目，以满足减少存储消耗，并节约许可的需求。
- 生成详细的数据访问和用户活动报告，帮助管理合规性。
  - » 按照用户名和IP地址跟踪客户数据的所有访问，以确保数据隐私策略的执行。
  - » 包括一个直观的报告引擎，该引擎不要求高级的数据库和报告编写技能。
  - » 提供透明性、可问责性和可测性，以满足法规的要求，撰写合规性报告。

2.2 QRadar Risk Manager

IBM® Security QRadar® Risk Manager有助于自动化任务关键型领域中的安全风险管理职能，加强对攻击的防御，同时提高合规性。IBM Security QRadar Risk Manager与IBM Security QRadar SIEM配合工作，根据事件和网络流量数据的上下文知识来识别漏洞和错误的防火墙配置，并确定其优先级。在结合使用时，这两种产品都可以帮助提高运营效率，降低风险并简化合规性活动。

IBM Security QRadar Risk Manager:

- 分析防火墙配置，帮助识别错误，并删除无效的规则。
  - » 执行详细的配置审计，以帮助提高防火墙规则的一致性，包括对隐藏规则和其他配置错误的检测。
  - » 通过对随着时间推移所发生的变化进行比较来执行审计，并提醒用户有风险的或违反合规性的配置。
  - » 通过识别未使用的或无效的规则，提高整体的防火墙性能。
- 提供网络拓扑结构和连接的可视化工具，查看当前的和潜在的网络流量模式。
  - » Topology Viewer使您能够查看网络设备和关系，包括子网和链接。
  - » Connection Monitor根据路由和防火墙配置提供网络配置的详细视图。
- 识别活动的攻击路径和高风险资产，以帮助降低风险并确定补救活动的优先级。
  - » 将网络上下文添加到资产和漏洞数据，使您能够确定补救活动的优先级。
  - » 模拟网络攻击，包括攻击在网络上的潜在传播。
- 支持网络流量、拓扑结构和漏洞风险的策略合规性监控。
  - » 使用自动化的策略监控程序实现多个安全政策的主动评估。
  - » 关联资产配置和漏洞数据与日志、事件和网络流量数据，以监测网络资产及设备。
  - » 支持审计要求和策略合规性报告，包含触发安全事故的异常、日志事件和电子邮件通知。

2.3 QRadar Log Manager

IBM® Security QRadar® Log Manager是一个高性能的系统，用于收集、分析、归档和存储大量网络及安全事件日志。该系统分析来自网络和安全设备、服务器和操作系统、应用程序、端点等的数据，对不断发展的威胁提供近实时的可见性。IBM Security QRadar Log Manager还可以帮助您满足合规性的监测和报告要求。

IBM Security QRadar Log Manager:

- 近实时地从数千个源捕获并处理大量事件数据，对不断发展的威胁提供可见性，并有助于满足持续合规监控的要求。
  - » 从多种网络和安全设备收集数据，包括路由器、交换机、防火墙、虚拟专用网络(VPN)、入侵检测/防御系统(IDS/IPS)、防病毒应用程序、主机和服务器、数据库、邮件和Web应用程序、自定义设备，以及专有应用程序。
  - » 分析和关联不同的日志数据和事件，对合规性风险、潜在的攻击、不适当的数据访问、内部威胁等提供切实可行的洞察。
  - » 使用可定制的仪表板实现基于角色的按职能访问，并提供近实时的和历史的日志数据的完整视图，包含合规性和威胁管理的大量报告。
  - » 向完整的IBM Security QRadar SIEM产品提供一个无缝的迁移路径，帮助简化从安全信息管理到真正的安全智能的过渡。
- 提供丰富的合规性报告功能，帮助满足或超越监管要求。
  - » 有助于满足法规遵从性的审计和报告要求，使用大量内置的关联规则和报告，以及自动报警，实现近实时的策略执行。
  - » 支持Payment Card Industry Data Security Standard (PCI DSS)、Health Insurance Portability and Accountability Act (HIPAA)、Gramm-Leach-Bliley Act (GLBA)、North American Electric Reliability Corporation (NERC)和Federal Energy Regulatory Commission (FERC)、Sarbanes–Oxley (SOX)等法案的要求。
  - » 在持续监控方面超出了Federal Information Security Management Act (FISMA)的要求，可以帮助政府机构制定基于风险的IT安全战略。
- 可扩展到在单个统一数据库中近实时地支持每秒数十万个事件。
  - » 采用的架构配置范围从集所有功能于一身的硬件或软件解决方案，到使用一个集中式控制台和任意数量的分布式事件处理器和事件收集器设备的企业部署。
  - » 每个设备为事件日志归档提供高达16 TB的容错存储，并且能够使用联合数据库架构扩展到数百个TB。
  - » 支持丰富的日志文件完整性检查，包括NIST Log Management Standard SHA-x (1-256)散列，以实现防篡改的日志归档。
  - » 包括一个可定制的事件索引功能，大大加快了自由文本检索。
  - » 允许用户按时间和数据类型自定义数据保留，以及压缩旧的数据，以进一步扩展事件数据保留功能。
- 提供高可用性和灾难恢复选项，帮助保持不间断的日志源数据收集和存储。
  - » IBM Security QRadar高可用性软件让您可以利用系统之间的自动故障转移和全磁盘同步，可在设备或服务器发生故障的情况下支持不间断的运行。
  - » 灾难恢复设备可以将日志数据镜像到一个完全相同的异地辅助备份系统，从而帮助您保护您的日志数据。
  - » 先进的即插即用设备可搭配使用IBM Security QRadar的任何元素，使您可以在需要它的时间和位置上添加保护。

2.4 网络活动收集器(Network Activity Collectors) (QFlow/VFlow)

IBM® Security QRadar® QFlow Collector结合了IBM Security QRadar SIEM与流处理器，提供第7层的应用程序可见性和流分析，以帮助您了解并响应整个网络中的活动。这项综合的解决方案为您提供了更大的网络活动可见性，可以更好地检测威胁，满足策略和法规合规性要求，并最大限度地降低对任务关键型服务、数据和资产的风险。

IBM® Security QRadar® VFlow Collector结合了IBM Security QRadar SIEM，对虚拟网络流量提供第7层应用层的可见性，以帮助您了解和响应整个网络中的活动。这项综合解决方案有助于支持VMware虚拟环境，实现对1000多个应用程序的分析；更好地检测到威胁；满足策略和法规合规性要求；并最大限度地降低对任务关键型服务、数据和资产的风险威胁。这项解决方案在虚拟服务器上运行，并且不需要额外的硬件。

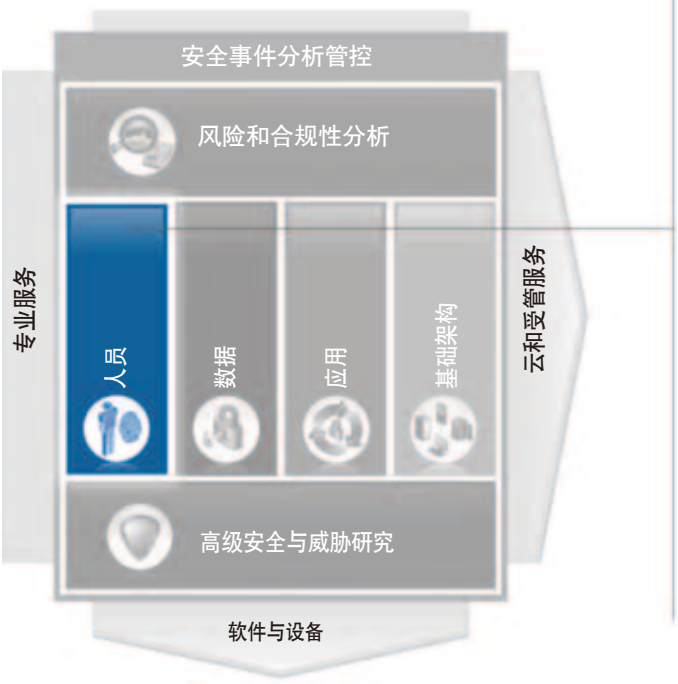
IBM Security QRadar QFlow/VFlow Collector搭配IBM Security QRadar SIEM提供:

- **威胁检测。**IBM Security QRadarQFlow Collector对应用程序级的网络流量数据使用深度包检测技术，无需依靠漏洞签名就可以发现新的安全威胁。您可以通过对所有网络流量(包括应用程序、主机和协议)的行为分析来识别恶意软件、病毒和异常。
- **策略与法规合规性管理。**您可以识别并纠正违反策略的行为；在非标准端口上运行应用程序；使用明文的用户名和密码登录到关键服务器的用户，以及在网络的敏感区域使用未加密协议。
- **社交媒体监控。**利用IBM Security QRadar SIEM和IBM Security QRadarQFlow Collector，您可以监控和分析在社交媒体平台和多媒体应用程序上的活动，以检测对您的网络的潜在威胁。利用近实时的异常检测和内容捕获功能，可以更容易检测到恶意软件，识别漏洞，并监控您的团队的社交通信(包括他们的使用模式)。
- **高级的事件分析和洞察。**您可以对应用程序流数据与从安全设备发送的日志事件执行近实时比较。日志和流数据之间的关联可以帮助识别通过其他方式可能无法发现的严重威胁。
- **持续的资产分析。**对网络上找到的新资产自动识别并进行分类，并发现它们正在运行的端口和服务。当添加新的系统或服务以及配置发生变更时，这些分析功能可以及时提醒。

人员安全

3

研究领域
利用全面的身份智能，跨安全域管理和扩展企业身份上下文



产品组合概述

IBM Security Identity Manager *

- 在整个生命周期中自动化用户的创建、修改和终止
- 身份控制，包括角色的管理和审计

IBM Security Access Manager Family *

- 自动化企业 Web 应用程序和服务的登录和身份验证
- 通过基于风险的访问检测和防止 Web 欺诈
- 细粒度访问执行的授权管理

IBM Security zSecure suite *

- RACF 之上的用户友好层，可以改进管理和报告
- 在大型机上监控、审计和报告安全事件、风险与合规性

精明的组织认识到，有效的身份和访问管理不仅仅是其安全结构的支柱，还是企业的一个迫切需求。毕竟，保护IT资产的访问并确保符合安全策略的能力可能会影响公司的竞争态势和盈利能力。今天的头条新闻讲述了这样一个故事：一个安全漏洞或失败的审计可能会以组织的声誉甚至收入损失为代价。随着IT基础架构的互联性变得更强，以及云采用率的增长，控制和监视用户的访问权限及活动变得更关键、更复杂。

IBM Security解决方案可以帮助组织降低未经授权的访问所带来的风险，并支持有效的Identity and Access Management(身份和访问管理)治理策略。同时，这些解决方案可以简化用户授权的管理，往往还伴随着可衡量的成本和时间节省，同时简化用户对受保护资源的访问。而且，这些解决方案还帮助组织应对移动工作人员和可信业内人士的安全挑战，这两组人往往对组织的信息的完整性和数据隐私性构成最大威胁。

IBM对Identity and Access Management的愿景是帮助客户在所有安全域管理企业身份，使用IAM作为一种工具，更好地管理新兴的安全威胁。这种方法扩展了IAM的作用，可向企业提供有价值的智能分析，同时在整个互联网的企业中执行用户对数据、应用程序和基础架构的访问。

IBM的Identity and Access Management产品和服务提供:

身份管理——让用户登录并分配访问权限，修改用户角色和权限，在用户生命周期结束时终止访问权限。

访问管理——提供用户的安全身份验证，包括单点登录(SSO)，一旦用户通过身份验证就马上执行访问策略。

用户合规性审计——监控、审计和报告用户活动，帮助组织促进对策略和法规的合规性，并通过监测用户的行为来减少内部威胁的风险。

3.1 IBM Security Identity Manager

IBM Tivoli Identity Manager是一个自动化的基于策略的用户配置解决方案，用于在整个IT基础架构内管理用户角色、身份和访问权。这一安全的身份管理软件能够让组织轻松部署使用，同时能帮助组织更好地遵守法规、管理风险和支持安全协作。

Tivoli Identity Manager可通过自动化、用户自助服务和其他创新来节省成本和提高生产力。

- 自动管理整个用户生命周期(从注册到终止)的角色、帐户和访问权。这项功能可以减少间接成本并消除人工错误。
- 通过预配置策略和模板加速新应用程序应用和用户注册。该软件可在数分钟而不是数天内为新用户提供所需资源。
- 提供自助服务界面，以便用户自行修改密码和个人信息。这可减少帮助成本并提高IT员工的效率。
- 建立职责分离以增强安全性与合规性。它可以结合各种需求，防止业务与管理用户访问权的角色和配置策略之间发生冲突。
- 通过定期纠正工作流程来纠正和去除不合规的访问权，或者通过基于角色的访问控制策略来实现。这一强大的功能可提供精密的、对审计人员友好的详细信息，以显示合规性。

3.2 IBM Security Access Manager产品家族

IBM Security Access Manager for Enterprise Single Sign-On

IBM Security Access Manager for Enterprise Single Sign-On(前身为IBM Tivoli® Access Manager for Enterprise Single Sign On)可以帮助降低服务台成本，提高生产力，并加强安全性。

- 利用新的虚拟设备简化部署和管理
- 为虚拟桌面和应用程序提供安全
- 利用对混合RFID智能卡和居民身份证的支持，提升强大的身份验证选择。
- 利用细粒度的审计日志、集中式审计和报告功能，促进其法规合规性
- 利用自动化登入/登出，并且对所有应用程序使用单一密码，从而简化用户访问
- 利用对网亭的全面会话管理或共享工作站环境，提高安全性和用户工作效率
- 由于密码重设电话更少，从而降低服务台成本
- 支持Microsoft Windows 7的64位平台和应用程序
- Epic适配器结合RFID徽章，可为医疗保健行业的客户提供无缝的单点登录，以及对Epic应用程序的即时访问。

IBM Security Access Manager for Web

IBM Security Access Manager for Web(前身为IBM Tivoli® Access Manager for e-business)将用户访问管理和Web应用程序保护综合在一个高度可扩展的用户身份验证、授权和Web单点登录解决方案中。IBM Security Access Manager for Web保障用户对在线应用程序的访问，并帮助保护他们不会受到先进的Web威胁。

IBM Security Access Manager for Web作为一个硬件或虚拟设备提供给组织，可以实现更简单的部署和更低的运营成本，可以解决关键的Web安全与合规性需求。单点的身份验证和会话管理使其更易于实现策略驱动的高级应用程序访问控制。

- **先进的威胁防护**——由IBM X-Force提供支持的IBM Security Web Gateway AMP 5100硬件设备在单个解决方案中集成了Web单点登录和身份验证、Web访问管理，以及对来自外部Web威胁的防护。

- **保护任何位置的敏感IT资产**——与IBM Security Access Manager for Cloud and Mobile的集成将用户访问保护扩展到移动环境和云环境中。
- **简化的配置选项**——虚拟或硬件设备的构成因素可以更快地实现价值并提供更高的投资回报。
- **大规模可扩展性**——较高的可扩展性、可用性等优秀性能可以实现单个实施中支持数百万用户。
- **统一的用户体验**——向跨不同Web应用程序和服务(包括IBM WebSphere®、Microsoft®、SAP和许多其他应用程序环境)的用户提供一致的Web单点登录(SSO)和登出。
- **应用程序兼容性**——集成在线业务应用程序，实现高度安全、统一和个性化的在线业务体验。

3.3 IBM Security zSecure套件

Security zSecure套件提供具有成本效益的安全管理，通过检测威胁改善服务，并利用自动化审计与合规性报告降低风险。

IBM Security zSecure Admin

这是在RACF之上的一个用户友好的层，在大型机上支持安全管理、用户管理与合规性管理:

- 定义访问权限并将其授予用户和用户组。
- 设置和重置用户的ID及密码。
- 显示一个用户ID或一个用户组的所有出现或交叉引用。
- 运行日报或月报。
- 在离线副本中对RACF数据库配置的变更进行测试。
- 帮助快速识别潜在的问题，以尽量减少安全漏洞的风险。
- 让高级管理员可以专注于更高价值的任务。
- 执行RACF数据库清理，以删除未使用的或过时的授权
- 产品前身为IBM Tivoli zSecure Alert
- 支持的操作系统: z/OS

IBM Security zSecure Visual

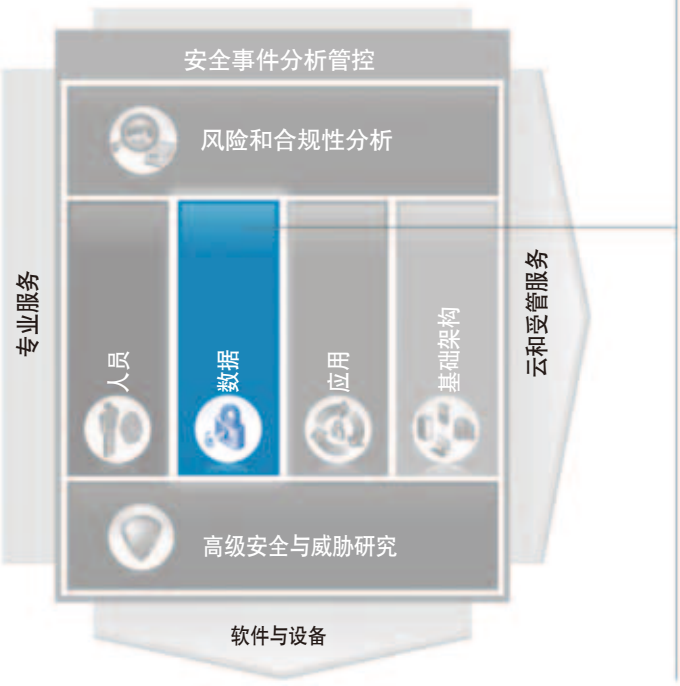
IBM Security zSecure Visual利用直接的、易于使用的图形化界面实现高效和有效的RACF® 管理，该界面使用的资源更少，但提供的功能更丰富。

- 使服务台的工作人员能够直接从一个易于使用的Microsoft Windows界面查看和管理配置文件。
- 利用分散的RACF管理来减轻高级IT人员的管理负担。
- 降低TSO/ISPF部署的成本和复杂性。
- 通过复制标准的用户模板，快速创建新用户
- 减少对高度专业化的RACF管理技能的需要。
- 通过限制管理权限范围，降低分散的RACF管理员的安全风险。
- 支持用户显示的站点自定义，以包括来自HR文件(如员工和部门编号)的数据。
- 产品前身为IBM Tivoli zSecure Visual。

数据安全

4

研究领域
企业范围的解决方案，帮助在您的数据中心保护可信信息的隐私性和完整性



产品组合概述

IBM InfoSphere Guardium产品家族

- Database Activity Monitoring——持续监控并阻止未经授权的数据库访问
- Privileged User Monitoring——检测或阻止数据库管理员、开发人员和外包人员的恶意或未经批准的活动
- Database Leak Prevention——帮助在数据中心检测和阻止泄漏
- Database Vulnerability Assessment——扫描数据库，检测漏洞并采取行动
- Audit and Validate Compliance——利用预配置报告和自动化的工作流简化 SOX、PCI-DSS 和数据隐私流程

IBM Security Key Lifecycle Manager

- 集中化和自动化加密密钥管理流程
- 利用直观的配置和管理用户界面简化管理

数据是全新的全球货币和企业的命脉。您是否知道数据库服务器是违规数据的主要来源？特别是在数据的数量、品种、速度和真实性都较高的时代中，组织如何能够确保合规性并保护自己免受恶意的内部袭击和外部攻击？答案是，建立一个全面的方法，在整个企业中保护结构化、非结构化、在线和离线的数据。IBM可以帮助您:

- 发现敏感数据并进行分类
- 利用屏蔽、加密和修订来保护数据
- 实时保护并连续监测数据访问
- 证明合规性，以通过审计
- 可通过扩展来保护物理、虚拟、云和大数据系统

4.1 IBM InfoSphereGuardium产品家族

InfoSphereGuardium Activity Monitor

IBM® InfoSphere® Guardium® Activity Monitor可监控所有事务，包括授权的数据访问和未经授权的数据访问。它可保护各种规模的数据中心，而无需更改数据库或应用程序，并且不会影响性能。InfoSphereGuardium Activity Monitor是针对大数据环境的监控和审计解决方案。

InfoSphereGuardium Activity Monitor提供:

- **深入所有数据活动的完整可视性**——针对所有平台和协议。
  - » 为您提供有关用户(包括数据库管理员、开发者和外包人员)和应用程序使用的所有平台和协议的所有事务的完整可视性。
  - » 识别从公共服务帐户(例如，Oracle E-Business Suite或PeopleSoft Enterprise)进行未经授权更改的应用程序用户。
  - » 提供独立于本机数据库记录和审计功能的用户和应用程序访问监控。
  - » 通过检测来自应用层的不寻常的数据库活动和更新活动来提高数据安全性。
  - » 自动执行敏感数据发现和分类。
- **监控和策略实施**——针对所有数据访问、更改控制和用户活动。
  - » 监控并实施敏感数据访问策略、特权用户操作策略、更改控制策略、应用程序用户活动策略和安全异常策略。
  - » 通过将数据活动与正常的行为基线进行比较，使用访问策略来识别异常行为。
  - » 基于可定义的阈值(例如，SQL错误)支持异常策略。
  - » 使用挤出(extrusion)策略来检验离开数据库的数据，以查找特定值模式(例如，信用卡号)。
  - » 支持基于策略的操作，例如近实时的安全警报、软件分块和用户隔离。
- **集中聚集审计数据**——针对企业合规性、报告和取证。
  - » 聚集整个企业的数据来进行合规性审计和报告、关联及取证，无需启用本机数据库审计功能。
  - » 提供防干扰的审计跟踪，支持审计员所需的职责分离。
  - » 交付可定制的合规性工作流程自动化，以生成合规性报告，并将报告分发给监督团队进行电子签名和升级。
- **广泛的异构支持**——针对所有主要的平台和操作系统，包括大数据环境。
  - » 监控并审计基于Hadoop的系统，例如，IBM InfoSphereBigInsights™ 和Cloudera。
  - » 支持企业数据库和操作系统，包括 IBM DB2®、Teradata、IBM Netezza®、Sybase、Microsoft SQL Server、UNIX和Linux。
  - » 支持关键的企业资源规划和客户关系管理应用程序，以及定制和打包应用程序。
  - » 提供在主要平台(包括Microsoft SharePoint)上跟踪文件共享活动的功能。
  - » 发现所有平台和协议的敏感企业数据并加以分类。

InfoSphereGuardium Data Encryption for DB2 and IMS Databases

IBM® InfoSphere® Guardium® Data Encryption for IBM DB2® and IBM IMS™ Databases 为 DB2 for IBM z/OS®和IMS数据系统提供加密。它使用IBM System z® 加密硬件来保护位于DB2行级别和IMS段级别的敏感数据。

InfoSphereGuardium Data Encryption for DB2 and IMS Databases可提供:

- **高级数据加密和解密**——实现数据安全性、隐私性和低开销。
  - » 使用z/OS综合加密服务设施提供DB2编辑例程和IMS出口例程，保护存储介质上的敏感数据。
  - » 使用三重数据加密标准、ANSI数据加密算法和高级加密标准算法。
  - » 支持您安全地使用存储区域网络，同时符合国际隐私和安全法规。
  - » 提供对访问数据库的应用程序透明的加密例程，无需更改应用程序。
  - » 提供指定加密密钥的功能。
- **交互式系统生产率设施(ISPF)前端和出口驱动程序**——用于优化效率、加密和压缩功能。
  - » 提供ISPF前端，允许您创建和定制加密、外部压缩和出口驱动程序。
  - » 提供出口驱动程序，在相同出口点允许压缩和加密，以避免影响现有压缩功能。
  - » 通过数据库重新装入期间使用的标准DB2和IMS出口例程更快实施。

InfoSphereGuardium Vulnerability Assessment

IBM® InfoSphere® Guardium® Vulnerability Assessment通过扫描数据库基础结构，检测漏洞并建议补救操作。该软件会检查诸如缺少补丁或者错误配置特权之类的风险。它还可通过近实时地监控所有数据流量，基于访问和操作数据的方式来识别漏洞。

InfoSphereGuardium Vulnerability Assessment帮助您消除由不安全的配置、强度较弱的密码和其他漏洞所引起的风险。

- **自动执行漏洞、配置和行为评估**——扫描整个数据库基础结构来寻找其中的漏洞。
  - » 包含预先配置的漏洞测试(围绕Center for Internet Security (CIS)和Security Technical Implementation Guide (STIG)最佳实践)，通过IBM InfoSphereGuardium知识库服务定期更新。
  - » 提供特定于平台的静态测试，检测正在评估的特定数据库的不安全配置。
  - » 执行动态测试来揭示行为漏洞，例如，账户共享、登录失败次数过多和不寻常的非营业时间活动。
  - » 不依赖于会影响系统可用性的入侵式利用或测试，并提供外部引用信息，例如，公共漏洞和暴露(CVE)标识。
  - » 支持主要的数据库平台和所有主要的操作系统，包括大数据环境。
- **报告和操作计划**——评估并记录数据库安全性，帮助您评价、升级和解决风险
  - » 生成详细报告和支持数据。
  - » 提供安全性评估摘要，其中包含加权度量和建议的补救操作计划来增强安全性。
  - » 集成了IBM InfoSphere Advanced Compliance Workflow Automation，能自动调度评估并管理报告分发、签名和升级。

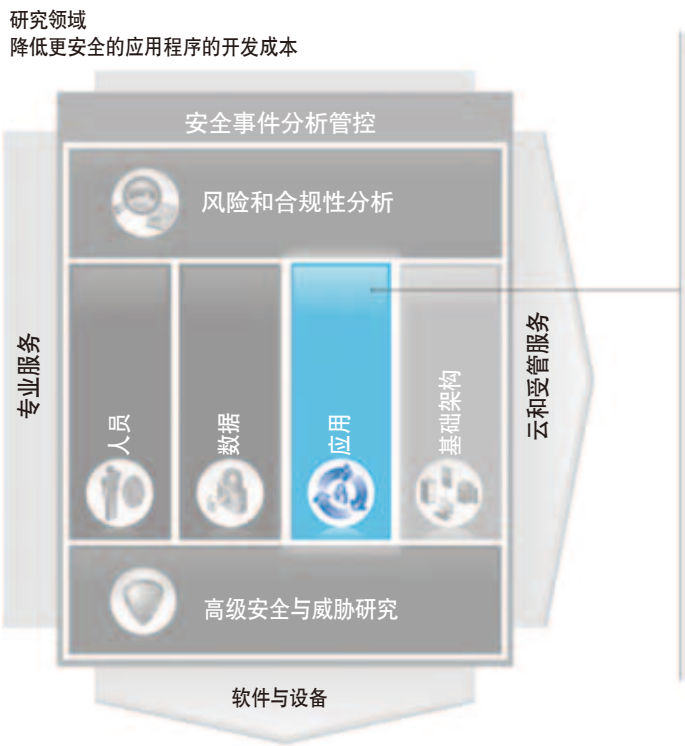
4.2 IBM Security Key Lifecycle Manager

IBM Tivoli® Key Lifecycle Manager支持IT组织集中和增强密钥管理流程，帮助其更好地管理加密密钥生命周期。

- 集中并自动化加密密钥管理流程
- 增强数据安全性，同时显著减少需要管理的加密密钥数量
- 借助用于配置和管理的直观的用户界面，简化加密密钥管理
- 帮助尽可能地减少丢失或破坏敏感信息的风险
- 帮助促进法规标准的合规性管理，比如Sarbanes-Oxley和Health Insurance Portability and Accountability Act (HIPAA)
- 将密钥管理功能扩展到IBM和非IBM产品中
- 利用开放标准，提高灵活性并促进供应商的互操作性

应用安全

5



产品组合概述

AppScan Enterprise Edition

- 利用治理和协作，实现应用程序安全测试和风险管理的企业级解决方案
- 多用户解决方案提供同时安全扫描和集中式报告

AppScan Standard Edition

- 桌面解决方案，为IT安全、审计师和渗透测试人员自动化Web应用程序安全测试

AppScan Source Edition

- 将源代码分析添加到AppScan Enterprise，支持静态应用程序安全测试

如今的组织依赖于移动和Web应用程序来吸引客户，提高员工的工作效率，并降低成本。如果没有适当的安全性，这些应用程序可能很容易受到安全漏洞的影响。最近的IBM X-Force®研究发现，去年有41%的安全漏洞与Web应用程序有关。

IBM Application Security解决方案使您能够在开发/运营生命周期的所有阶段中构建保护层，从而帮助您交付和维护安全的移动及Web应用程序。市场领先的应用程序安全性测试工具使您能够在开发流程中更早地找出漏洞并进行修补——降低构建安全和兼容的Web及移动应用程序的成本。一旦将应用程序部署在生产中，网络和数据库安全性的补充解决方案可针对内部和外部的威胁提供更多应用程序防御。与IBM安全智能工具的集成提供了应用程序安全性的各个方面的统一视图，并将网络、主机和数据的安全性考虑在内。结果会形成一个整体的角度，使您能够实施有效措施来保护您的应用程序，并提高组织的更广泛的安全性和风险状况。

IBM目前在Static Application Security Testing(静态应用程序安全测试)和Dynamic Application Security Testing(动态应用程序安全测试)的Gartner魔力象限中均位于领导者象限。

IBM Application Security解决方案提供:

- Static Application Security Testing(SAST，静态应用程序安全测试)在源代码中识别并修复Web和移动应用程序的漏洞
- Dynamic Application Security Testing(DAST，动态应用程序安全测试)在实时和预生产应用程序中发现Web和移动应用程序的漏洞
- 自动化静态和动态分析结果的关联
- 来自IBM Security Application Security Research团队的业界领先的功能，如玻璃盒测试(一种Interactive Application Security Testing(IAST，交互式应用程序安全测试)形式)、JavaScript Security Analyzer(JavaScript安全性分析器)和Cross-site Scripting Analyzer(跨站点脚本分析器)，这些对关键的应用程序安全挑战可以提供更加有针对性的分析。
- 支持传统应用程序的现代化，包括COBOL和SAP应用程序的源代码分析
- 通过IBM Security AppScan、IBM Security Network IPS、IBM Guardium和QRadar Security Intelligence Platform在整个开发/运营生命周期中融入全方位、多层次的保护

5.1 IBM Security AppScan产品家族

IBM为移动和Web应用程序提供一个市场领先的应用程序安全性和风险管理解决方案组合。凭借先进的安全性测试和一个管理应用程序风险的平台，IBM Security AppScan(前身为IBM Rational AppScan)产品组合提供专业知识和关键的应用程序生命周期管理，以及必要的安全平台集成，使企业不仅能够识别应用程序漏洞，也可以降低整体的应用程序风险。IBM Security AppScan产品组合包括动态应用程序安全测试(DAST)和静态应用程序安全测试(SAST)，以及创新的技术(如玻璃盒测试和运行时分析)，这些产品与最新的威胁保持同步，并推动精确的、切实可行的结果。

AppScan Enterprise Edition

IBM® Rational® AppScan® Enterprise Edition是一个Web应用程序漏洞测试和报告解决方案，将安全性测试扩展到了整个企业。这项解决方案促进了信息安全性、开发和管理之间的沟通和协作。Rational AppScan Enterprise Edition有助于防止未经测试的Web应用程序和合规性问题给企业带来风险。Rational AppScan Enterprise Edition可交付:

- **战略性Web应用程序安全**——针对Web应用程序安全采取战略性方法。
  - » 向组织提供安全和法规遵从性风险Web解决方案可视化。
  - » 允许扩展审计活动，确保Web应用程序已经过测试。
  - » 组织能够吸引、培养、并开发质量保证(QA)团队，并在整个软件开发生命周期内实施安全性控制以减轻风险并降低成本。
  - » 使用测试技术组合提供彻底的自动化评估。
  - » 提供适合每个利益相关方的协作功能和工具。

- **全面扫描功能**——同时扫描和测试成百上千个应用程序并且频繁对其进行重新测试。
  - » 提供可扩展的企业架构，支持同时扫描多个应用程序。
  - » 及时扫描网站中嵌入的恶意软件以及指向恶意或不良站点的链接，确保您的网站不会使访问者感染病毒或在其不知情的情况下将其引导至不期望的或危险的站点。
  - » 关联使用动态和静态分析技术发现的结果。
  - » 测试Web服务。
- **企业级报告**——使用Web界面和企业报告能够轻松沟通安全性状态和特定问题。
  - » 清晰展示由已确定的安全性问题导致的安全性和合规性风险。
  - » 通过性能指标和趋势分析显示进度。
  - » 提供灵活的详细安全性问题报告，使用户能够以多种方式对其报告数据进行分类和组织。
  - » 交付40多种安全合规性报告，包括PCI数据安全标准(PCI DSS)、支付应用数据安全标准(PA-DSS)、ISO 27001和ISO 27002、HIPAA、GLBA及Basel II。
  - » 帮助强制执行测试策略，并通过基于角色的报告访问权和扫描许可权提供监管。
- **补救**——依靠发布公告以有效的补救措施来帮助指导开发者。
  - » 交付公告、修复推荐和内置培训视频，便于在识别和验证安全漏洞后实施补救过程。
  - » 提供问题管理功能，并与缺陷跟踪系统集成。

AppScan Source Edition

IBM® Rational® AppScan® Source Edition软件通过扫描和检测应用程序源代码中的漏洞，将安全性测试集成到软件开发生命周期中。现在，您可以及早地减少开发生命周期中的漏洞、评审数据流并识别每个应用程序面临的威胁。

此静态分析安全性测试解决方案支持以下功能:

- 通过全面的源代码分析方法，增强应用程序安全性。
  - » 在应用程序生命周期的较早阶段，识别源代码中由安全性缺陷产生的数据违规风险的根源并予以纠正。
  - » 在构建过程中通过集成安全性源代码分析与自动化扫描，在开发过程中构建自动化的安全性。
  - » 对安全性策略进行扫描、分类和管理；确定向安全性团队分配结果的优先次序以进行漏洞修复。
  - » 每小时对一百多万条代码行进行快速扫描，甚至允许您扫描最复杂的企业应用程序。
  - » 使用字符串分析来简化开发团队进行安全性测试的过程。
- 与现有应用程序进行集成，如应用程序开发与当前使用的安全性应用程序。
  - » 容纳涉及大量语言的大型复杂应用程序的广泛组合。
  - » 基于开放式架构的构建，可保护您的现有投资。
  - » 与缺陷跟踪系统(DTS)、软件配置管理和构建管理工具、动态分析工具以及Web应用程序防火墙进行集成。

- 通过支持遍及整个企业的一致性策略改善合规性。
  - » 允许您设置、推动和执行可在整个企业中使用的一致策略。
  - » 通过集中的策略和评估数据库，提供企业级指标和报告。
  - » 在整个软件开发生命周期中，更方便您基于审计和合规性目的，从主管级别出发，了解自身所面临的威胁。

AppScan Standard Edition

IBM® Rational® AppScan® Standard Edition可自动执行漏洞测试，帮助抵御网络攻击威胁。该解决方案将动态分析与静态JavaScript分析相结合，用于在生产前后测试和审计Web应用程序。

Rational AppScan Standard Edition支持:

- **全面的覆盖范围**——针对广泛的应用程序漏洞提供扫描和测试功能。
  - » 针对新出现的Web漏洞自动执行动态(黑匣)安全性测试，包括Web服务、Web 2.0和丰富因特网应用程序，如JavaScript、Ajax和Adobe Flash。
  - » 包括JavaScript Security Analyzer，用于对客户端安全性问题进行高级静态(白匣)分析，如基于DOM的跨站脚本和代码注入。
  - » 增强了对Web服务和面向服务架构(SOA)的支持，包括SOAP和XML。
  - » 通过Rational AppScaneXtension Framework提供定制和可扩展性，允许用户社区构建和共享开放源码插件。
- **准确扫描和高级测试**——交付高级别的扫描准确性和先进的测试实用程序。
  - » 扫描网站中嵌入的恶意软件以及指向恶意或不良站点的链接。
  - » 通过特定于扫描的描述和针对每个问题的说明，简化扫描结果的解释过程。
  - » 包含自适应测试过程，可智能地模仿人类逻辑，使测试阶段适用于不同应用程序。
  - » 了解应用程序，向下深入到每个特定参数级别，然后进行调整以仅执行相关的测试。
  - » 包含高级测试实用程序，通过将Rational AppScan的功能与Pyscan脚本相结合，实现更为强大且更有效的手工测试，扩展了定制的安全性测试。
- **快速纠正**——通过排列优先次序的结果和修复建议快速纠正问题。
  - » 通过对每次扫描发现的漏洞提供完全排列优先次序的列表来简化纠正过程，这样可以最先纠正高优先级的问题。
  - » 说明纠正问题所需的步骤，包括安全和不安全代码的示例。
  - » 生成高级纠正功能，包括便于修复漏洞的全面任务列表。
  - » 与缺陷跟踪系统(如IBM Rational ClearQuest® 和HP Quality Center)集成。
- **增强的洞察力和合规性**——帮助管理合规性并获得对主要问题的洞察。
  - » 包含具有40种可供使用的合规性报告的法规遵从性报告模板，包括PCI数据安全标准(PCI DSS)、支付应用数据安全标准(PA-DSS)、ISO 27001和ISO 27002及Basel II。
  - » 通过持续支持应用程序安全性来帮助满足关键的合规性标准，如PCI DSS。
  - » 支持IBM Rational AppScan Reporting Console，为您提供关于风险的企业级可视性并不断更新纠正过程。

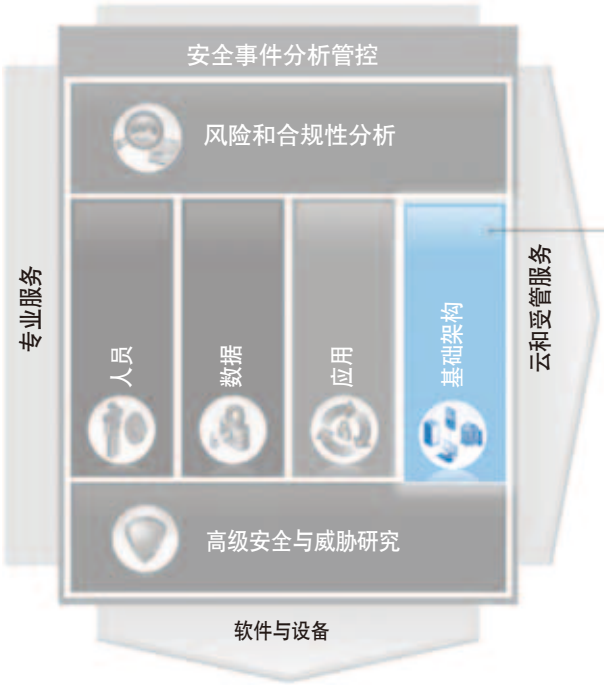
基础架构

6

基础架构(网络和端点)

研究领域

帮助针对复杂的攻击提供防范，并提供对用户、内容和应用程序的洞察。
维护持续端点合规性，同时降低管理分布式环境的成本与复杂性



产品组合概述

IBM Security Network Intrusion Prevention (IPS)

- 提供先进的威胁检测和防护，以帮助阻止对高价值资产的有针对性攻击
- 利用 IBM Virtual Patch® 技术主动提高防护能力

IBM Endpoint Manager for Security and Compliance

- 利用持续的闭环流程，有效地管理合规性生命周期
- 对安全配置和补丁提供准确的实时可视性，并持续执行安全配置和补丁
- 集中管理可以提供先进的防病毒和防火墙保护的功能

IBM Endpoint Manager for Core Protection

- 保护物理和虚拟端点避免受到病毒、木马、蠕虫等所造成的损害，集成的数据丢失防护 (DLP) 执行安全策略，并遵从数据隐私法规

IBM Endpoint Manager for Mobile Devices

- 利用先进的安全性与合规性特性保护企业数据
- 利用员工和企业拥有的设备的整合库存，获得企业可视性
- 从一个统一的基础架构进行管理，使用单一平台来管理所有企业设备

IBM Security Host Protection

- 结合个人防火墙、由 X-Force 研究机构提供支持的业界领先的入侵防护，以及文件和系统的完整性监控

IBM基础架构防护解决方案跨网络、服务器、虚拟服务器、大型机和端点提供深入的安全性。这涵盖了广泛的关键安全需求，从识别和拦截最新出现的威胁，到保持所有端点持续遵守组织策略。

IBM的Advanced Threat Protection Platform (ATPP)提供了一个可扩展的方法，可以快速响应当今不断发展的威胁环境。

端点安全性

IBM端点安全性提供实时可见性并自动化纠正操作，以保持所有端点都持续遵守组织的策略，这些端点包括服务器、PC、笔记本电脑、智能手机、平板电脑和专用设备(如销售点(POS)设备、ATM和自助服务亭)。当威胁出现时，这个IT运营端点管理和安全管理的统一解决方案可以让您迅速修复、保护并实时报告端点。

网络安全

IBM网络安全解决方案有助于保护整个网络基础架构避免受到网络层和应用层中不断发展的威胁。该解决方案的核心是IBM的网络入侵防护设备，该设备能够提供由IBM X-Force Research and Development Team提供支持的不断演变的防护。通过将积极的安全性研究集成到IBM的入侵防护解决方案中，IBM能够确保组织在暴露于新的安全威胁之前得到保护。

大型机安全

IBM大型机安全解决方案提高大型机平台的效率和可管理性，许多组织的任务关键型应用程序、生产系统和分类的业务数据都驻留在大型机上。IBM Security zSecure解决方案提供了全面的功能，以简化管理、执行安全策略、监控安全活动、检测潜在的威胁、发出实时警报、修复风险、自动化审计报告，以及自定义合规性报告。

6.1 IBM Security Network Intrusion Prevention (IPS)

IBM Security Network Intrusion Prevention System (IPS)旨在互联网安全威胁影响您的业务之前将其阻止。该软件可保护网络、服务器、桌面和Web应用程序，以抵御恶意威胁。通过为平台提供端到端的安全性聚合，可将成本高昂的点解决方案需求最小化。

IBM Security Network IPS可满足业内领先的入侵预防技术要求。

- **性能**——在受到影响前阻止安全威胁，而且不会降低高速网络性能。Security Network IPS可提供高吞吐量、低等待时间和快速正常运行时间，以维持高效的网络运营。
- **安全性**——利用其模块化产品架构，Security Network IPS可随着安全威胁的出现添加整套全新的保护模块。从蠕虫、僵尸网络、数据安全到Web应用程序，它可提供连续性、数据安全与合规性保护。
- **可靠性**——提供高可用性(主动/主动或主动/被动)、热插拔冗余电源和热插拔冗余硬盘，以帮助维持网络流量。
- **部署**——此架构无需重新配置网络易于部署。该软件可提供三种操作方式和改进的本地管理接口，以简化基本策略配置管理。
- **管理**——利用IBM代理的简单、强大的控制能力集中实现安全性管理。Security Network IPS提供完整的报告、事件相关描述和综合警报。
- **置信度**——作为入侵检测和预防的领军企业，IBM已建立了顶级客户支持记录。IBM X-Force研发团队是全球最知名的商业安全小组之一。

6.2 IBM Security SiteProtector

IBM Proventia® Management SiteProtector™ 系统提供了一个更简单、更具成本效益的方式来管理安全解决方案，并提供一个中央管理点来为您的企业控制实施安全策略、分析、告警和报告，从而简化法规合规性。

- 通过对不同的网络和主机安全设备采取中央控制，从而降低安全管理的成本和复杂性
- 通过事件分析和灵活的可定制报告，改善风险沟通
- 通过与现有系统集成，充分利用现有的投资
- 提供扩展的灵活性，以支持安全产品的更多类型和功能
- 使用预定义的模板轻松地创建报告
- 通过对比两个不同时间段内的资产漏洞，证明漏洞差异

- 利用内置的过滤和排序选项，执行基本的自定义
- 设置权限，只允许用户生成和查看面向指定的组的报告
- 导出为PDF、HTML和CSV格式
- 每天、每周、每月或在非高峰时间运行的调度报告
- 查看的报告涵盖工作流的工作单报告、内容及电子邮件过滤报告，以及病毒活动报告
- 通过控制台之外生成额外的响应(如电子邮件或SMTP)来升级重要事件，也可以通过降低警报优先级或选择性地阻止事件被显示或记录，从而降低对非重要事件的重视程度。
- Transfer SiteProtector在发生灾难性故障、网络中断或影响主站点的灾难时，将管理系统功能集中到辅助站点
- 支持的操作系统: AIX、i/OS家族、Linux、其他操作系统、Windows家族、z/OS

6.3 IBM Security Endpoint Manager

IBM Proventia® Desktop Endpoint Security帮助保障您的台式机和笔记本电脑的安全，不受已知和未知攻击的影响，在单一代理内提供多层安全性。旨在与您现有的基础设施轻松整合，这项多层端点安全性解决方案在单一代理内整合了个人防火墙、入侵预防、缓冲区溢出攻击预防、应用程序保护和病毒预防。

- 同时降低已知和未知类型攻击的风险
- 在单一代理内提供多层安全性
- 帮助确保遵从性，简化管理
- 帮助预防导致数据盗窃的攻击类型
- 版本10使用Microsoft Windows Vista 32位操作系统提供对端点的专门保护

”IBM安全解决方案”通过一个全新的安全智能框架，能够帮助组织真正实现IT安全管理，还有行业服务专家针对不同需求定制整合安全解决方案，帮助组织降低总体拥有成本。因此，无论风险是来自高级威胁、移动访问，还是云架构、合规性问题；或者组织正在力求通过分析大数据获得安全洞察，那么，来自IBM安全解决方案的工具和专家都可以协助她们积极实现。