安全、风险管理与合规性

Pulse2010

议程

- 欢迎致辞
- 智慧地球上的安全状况
- 深入了解：
  - 身份与访问安全性
  - 数据与应用程序安全性
  - 数据中心与运营安全性
- Pulse 2010大会的安全性、风险与合规性主题

Pulse 2010大会——安全性

- 在多个会场（安全性、中端市场、云计算、热点问题等）举行29场以安全性为主题的会议；
- 30位同行（IBM 客户）就安全性问题发表演讲；
- 演示大厅中8场以安全性为主题的演示；
- 超过45位专家现场解答您的问题；
- 18个实际操作实验室。

自上次相聚到现在…

162

我们已经与数百家新客户合作，建立了新的客户参考

500

通过收购Ounce Labs和Guardium，获得了500家客户

1260亿

每年为客户管理超过1260亿的事件

2

2份主要的安全性蓝图及指南文件，赢得了客户的称赞

95

95次新产品与服务发布与整合

4924

为客户保护4924个新漏洞

为什么选择IBM?
IBM在安全性方面有着独一无二的发展前景

IBM

值得信赖的顾问	安全性公司	解决方案提供商	IBM公司
帮助客户建设智慧城市、智慧电网、新型数据中心、可靠的通行证系统等。	提供各种安全产品与服务的领先软件及服务提供商	全球领先的软件与硬件解决方案提供商	在全球130个国家拥有400，000名雇员，并提供私有数据保护

IBM安全解决方案

智慧地球上的安全状况

我们的星球正在日益变得
物联化、互联化与智能化。

新的　可能性。

新的　复杂性。

新的　风险…

我们已经看到，在过去10年间所发生的变化已经超过了过去90年的变化。

Ad J. Scheepbouwer
KPN Telecom 首席执行官

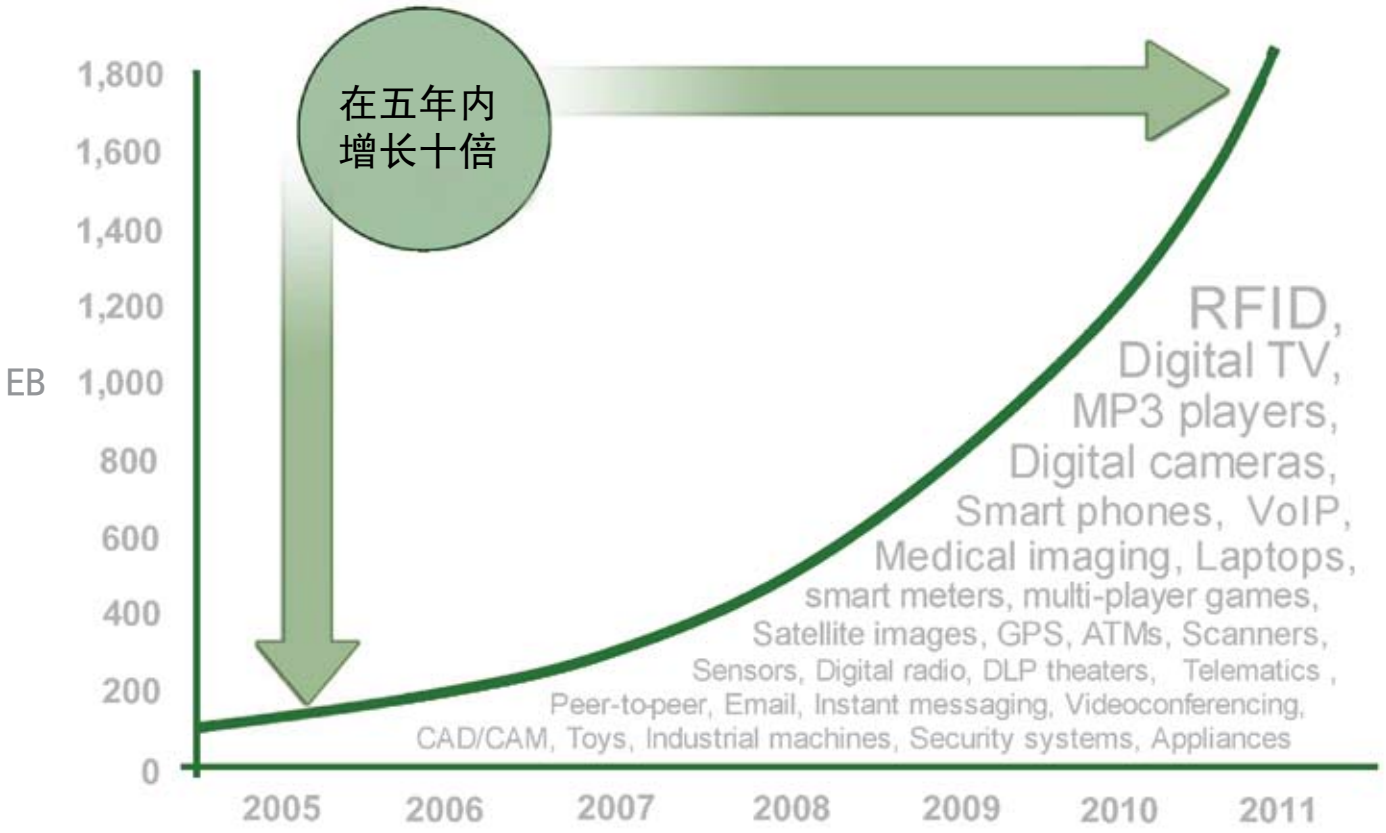
关键基础架构保护

隐私与身份

新型和新发的威胁

云安全

在短短的5年后，世界的物联化程度将增长10倍。通过互联网连接的设备将从5亿台飞跃至1万亿台。



大约70%的数字世界是由个人创建的，但是，在数据的安全、隐私、可靠性及合规性方面，企业承担了85% 的责任。*

*“随着经济紧缩，数字世界在膨胀”，IDC，2009年5月

有太多的方案需要规划…

	外部威胁	
	■ 电力故障	
无心的	■ 自然灾害 ■ 经济动荡	■ 恶意软件 ■ 拒绝服务 ■ 精心筹划的、有组织的攻击
	■ 未打补丁的系统 ■ 法规与应用程序漏洞 ■ 缺少变化控制措施 ■ 人为错误或者疏忽大意	■ 开发人员创造的后门 ■ 信息盗窃 ■ 内部欺诈
	内部威胁	故意的

同时，安全不再是一种选择，而成为一种需求…

为汽车设计的安全带

“现代机械化“，
Circa，20世纪30年代

设计用于将乘客稳固地固定在座椅上，这样，一旦发生事故，乘客不会被从车内甩出去。一款新研制的汽车安全带即可消除由此而造成的人身伤害。

座位安放在柱子上

婴儿在自制扶手椅中乘坐汽车

没有任何一款适合汽车使用的普通悬带型婴儿座椅能够让康涅狄格州托灵顿的Lester Bresson的小儿子满意，因此，父亲设计出了如左图所示的扶手椅。这把扶手椅是采用废旧木材、钢条以及废弃的装饰布制成的，扶手椅安放在汽车两个前排座椅之间底板上的柱子上。

系上安全带，否则等待违约通知单

- 2010年，法规日益要求“通过设计提高安全性”。
- 类似于汽车工业领域内安全标准的演变情况。

整合服务管理在整个业务基础架构范围内提供了可视化、可控化及自动化…

整合服务管理

针对各行业

凭借行业独一无二的架构、功能和专家经验，对包括IT在内的技术基础架构进行整合式管理，帮助企业向客户交付创新服务。

用于设计与交付

凭借专家经验和能力，将软件设计、交付与管理的一体化流程融入智能设备和服务的设计之中，帮助客户实现产品与服务的创新

用于数据中心

凭借专家经验和能力，协助客户在提升IT运行效率的同时，改善下一代数据中心IT交付和管理业务服务的效率和效益

…向客户交付创新产品与服务

IBM以整体的方式实现安全性，端到端覆盖了安全的基础

改善服务、管理风险并削减成本

智慧的安全：支持客户创新

智慧是

Gruppo Intergea：

减少和预防网络中断，改善连续性。识别并阻止新的未知威胁，实现卓越性能

智慧是

Northwest Hospital and Medical Center：

为实际访问与通过计算机访问重要的记录引入RFID标签，从而在医院及各个部门实现大幅度成本节约并提高效率。无需共享密码，使得机器与应用程序永久处于登陆状态…满足HIPAA要求

智慧是

缩短新的安全服务的面市时间

DTCC：

每年，超过225个应用程序中设计并内置了安全功能。提高了应用程序开发人员的生产力，并且缩短了每一项新服务的上市时间。

为什么选择IBM?
IBM Research，X-Force

IBM 安全性研究中心

IBM X-Force® 数据库

专门对如下内容进行了分析：

- 漏洞和利用
- 恶评/不良网站
- 网络垃圾与网络钓鱼
- 恶意软件
- 其他新趋势

来源：IBM X-Force数据库

世界上最全面的漏洞数据库

- 录入日期可追溯至20世纪90年代

由专门的研究小组每日更新，目前可跟踪：

- 7,600家厂商
- 17,000种产品
- 40,000个版本

IBM安全框架

赋予适当的用户在适当的时间访问适当的资源的权利；

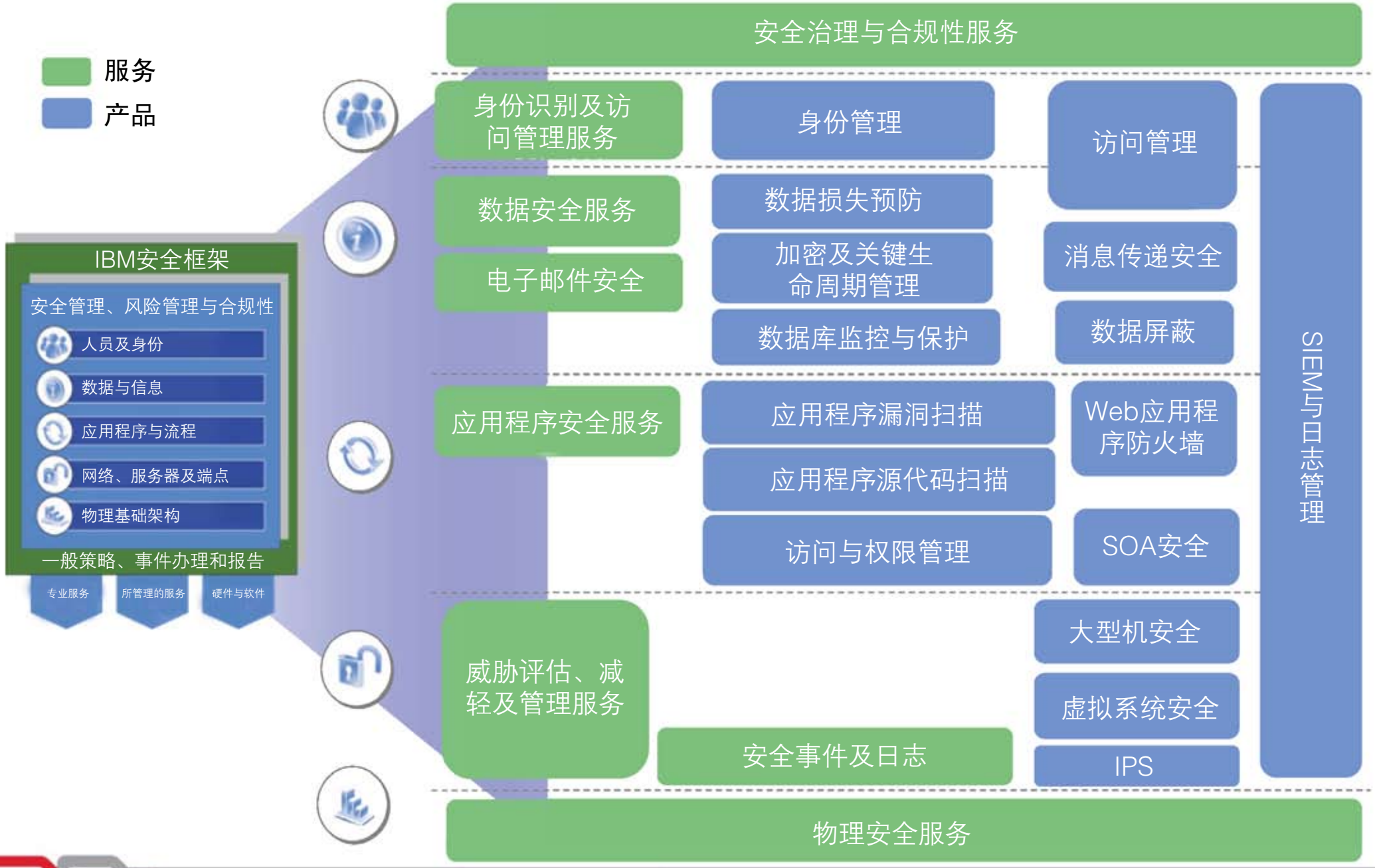
保护敏感的业务数据；

保持应用程序的可用性并避免恶意或者欺诈使用。

通过减轻风险的方式来优化服务可用性。

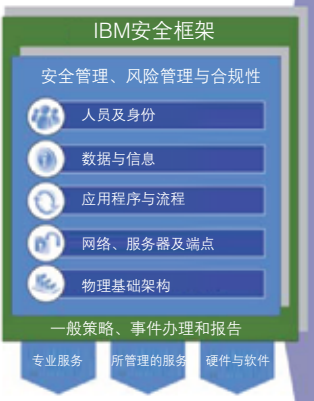
提供实用的洞察并改善物理基础架构安全的有效性。

IBM安全性产品组合


服务
产品
安全治理与合规性服务
身份识别及访问管理服务
身份管理
访问管理
数据安全服务
数据损失预防
消息传递安全
电子邮件安全
加密及关键生命周期管理
数据屏蔽
数据库监控与保护
应用程序安全服务
应用程序漏洞扫描
Web应用程序防火墙
应用程序源代码扫描
访问与权限管理
SOA安全
威胁评估、减轻及管理服务
大型机安全
虚拟系统安全
安全事件及日志
IPS
SIEM与日志管理
物理安全服务
IBM安全框架
安全管理、风险管理与合规性
人员及身份
数据与信息
应用程序与流程
网络、服务器及端点
物理基础架构
一般策略、事件办理和报告
专业服务
所管理的服务
硬件与软件

IBM安全解决方案

改善服务、管理风险并在不影响性能的情况下降低安全成本



身份与访问安全

授权适当的人员在适当的时间以有效、合规的的方式访问适当资源

数据安全与应用程序安全

从浏览器到硬盘，保护业务数据和事务的完整性和机密性

数据中心与运行安全

在降低风险的同时优化专长、技术与流程，从而优化服务可用性。

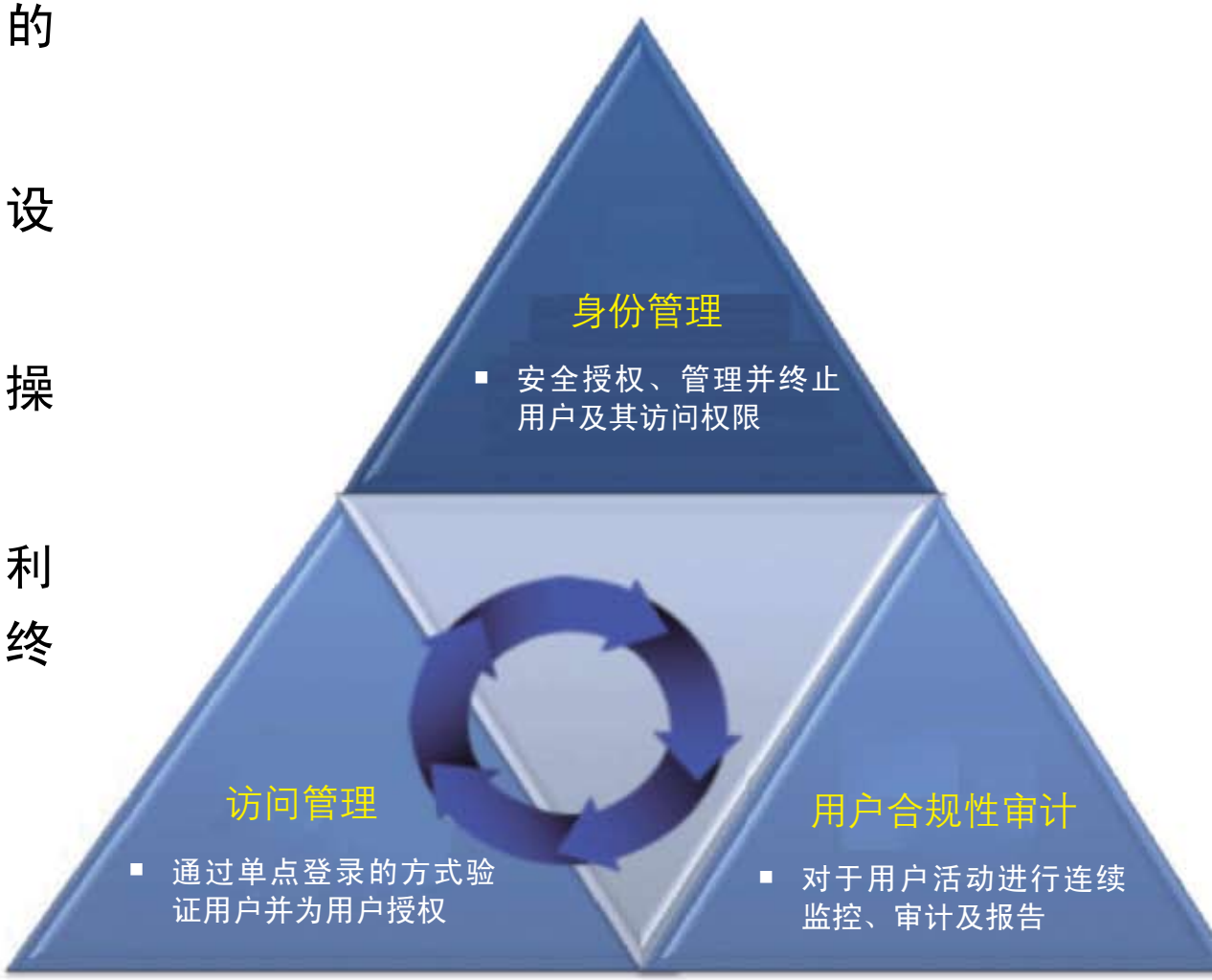
有关新产品的信息旨在简要介绍我们大致的产品方向，消费者不应以此为依据制定购买决策。新产品信息仅以提供信息为目的，不得纳入任何合同。新产品信息不表示我公司承诺、保证或者有法定义务提供任何资料、代码或者功能。针对我公司产品所描述的特性或功能的开发、发布及时间安排均由我公司自行决定。

数字身份管理的挑战

- 利用未使用的ID或者共享身份，对资源进行非正常访问
- 管理用户和身份的内部成本
- 特权用户活动未受监控
- 满足合规性要求，响应审计需要

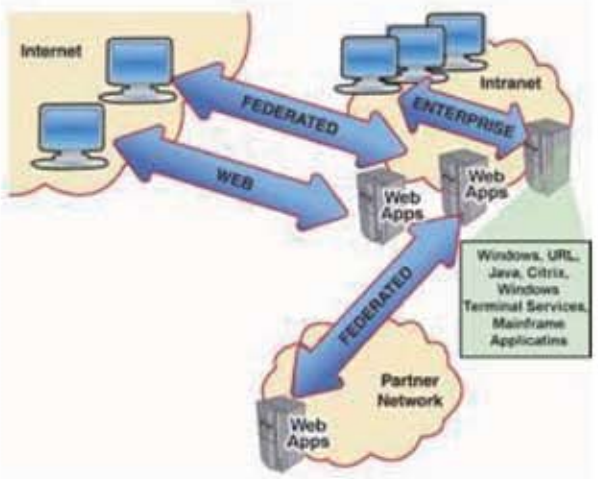
实现身份管理与访问管理能够解决这些挑战，驱动积极成果

- 能够将登录及取消身份识别的时间从数周降低至数分钟。
- 能够大幅降低帮助台密码重设呼叫产生的成本。
- 降低内部欺诈、数据泄露或操作中断的风险。
- 通过启用单点登录等活动，利用Web的业务应用来改进最终用户体验。

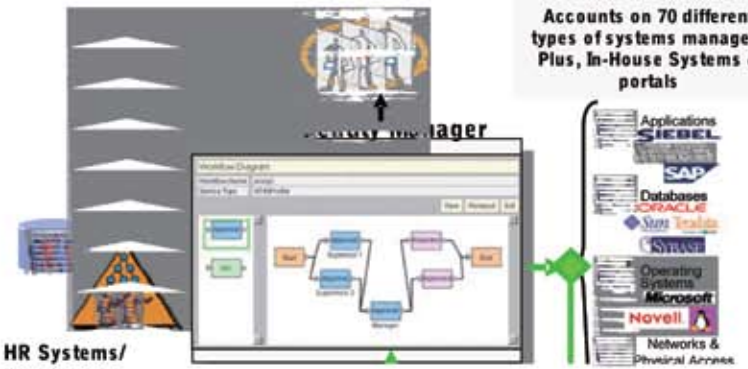


从身份与访问安全开始

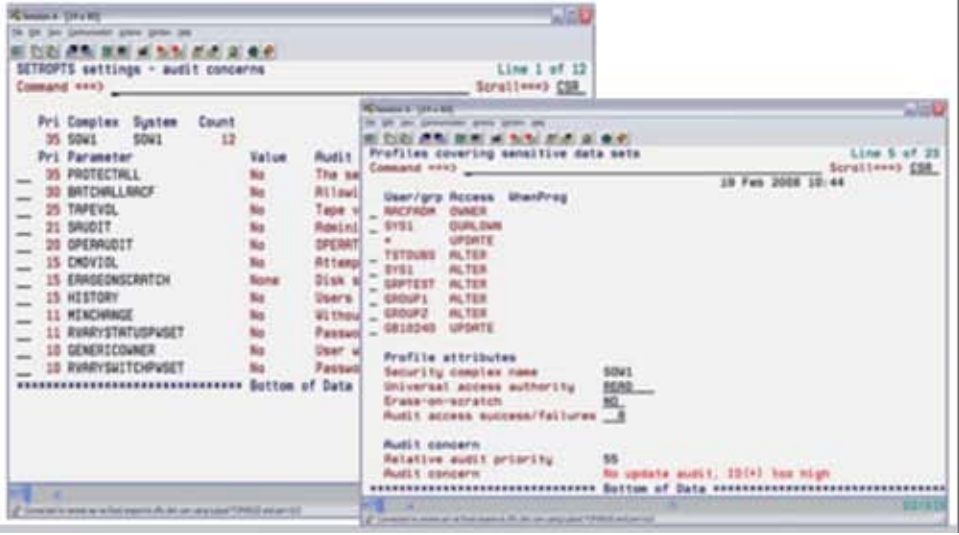
单点登录与
密码管理



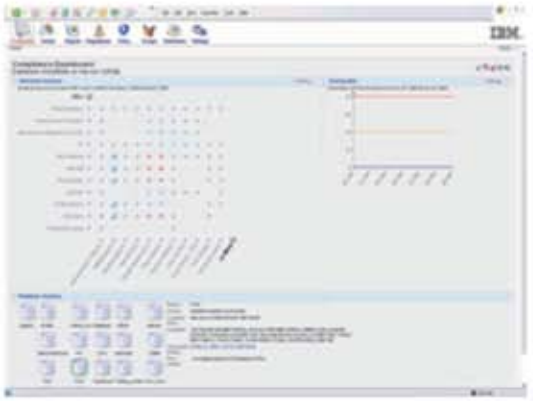
用户配置/角色管理



易于解释的大型机审计风险



安全日志管理存储与报告



IBM身份与访问安全

策略：

通过将身份识别的上下文拓展至应用程序、数据以及威胁管理，为客户增加价值

创新与集成的重点领域

- 扩展IAM治理功能
- 降低运营成本
- 进一步使得System z能够发挥企业安全中枢的作用。

市场驱动因素

简化	合规性	虚拟化	应用程序与数据保护

数据与应用程序保护面临的挑战

- 数据泄露与隐私合规性；
- 需要整合到企业内部的控制点的数量及复杂性；
- 数据泄露的成本、通知、品牌价值；
- 控制适当的人员在适当的时间访问适当的数据
- 应用程序安全性及敏捷性；
- 保护知识产权与在用数据；
- 确保机密数据安全。

可靠的数据及应用程序安全战略将跨越人员、流程及技术

- 集中式密钥管理；
- 组织间的数据收集；
- 集中式、细粒度的信息访问控制；
- 数据使用情况的审核与报告；
- 安全日志管理；
- 集中式服务器管理的完整性，包括虚拟服务器；
- 应用程序与数据库安全性。

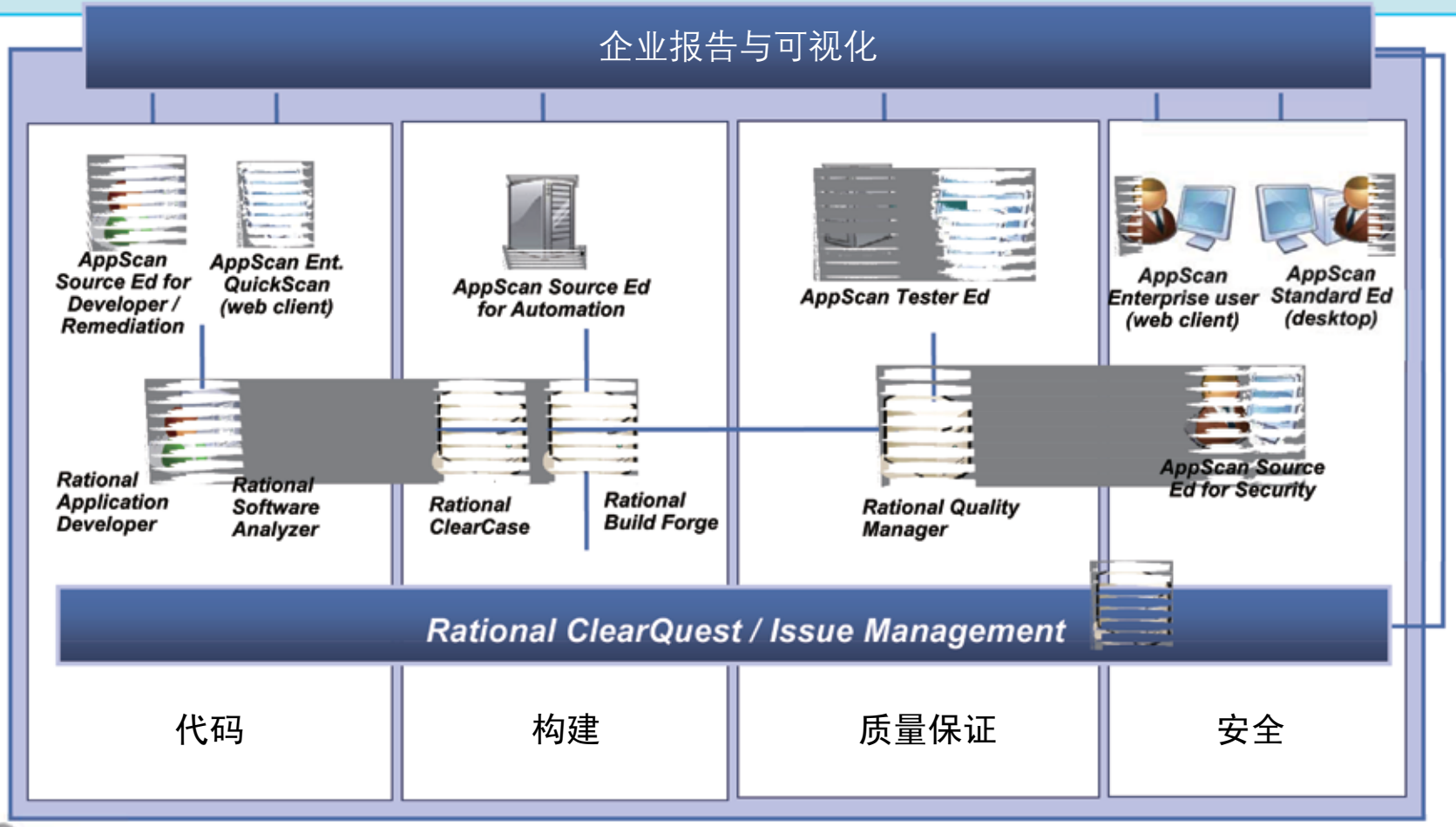
IBM已经收购了Guardium，该公司是防护数据库并保护关键企业数据领域的市场领军者

- IBM公司收购Guardium，使得我们的客户能够通过监控与保护高价值企业数据库确保信息基础架构值得信赖。

- 解决方案：Guardium实时数据库监控平台
  - 实时、自动化跨数据库管理系统（DBMS）的监控与审计平台；
  - 保护高价值数据库的安全并识别出应用层欺诈；
  - 能够始终如一地执行政府政策；证明合规性；
  - 与传统数据库管理系统审计相比，能够降低确保合规性所需成本及努力，同时，对当前业务流程不会带来任何影响。

收购Ounce Labs后，提高了安全测试的可操作性水平

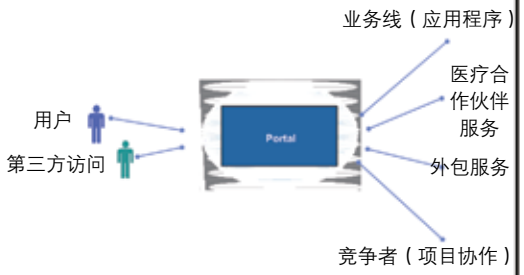
- 通过整合Ounce Labs源代码测试与IBM Rational AppScan应用程序安全测试，IBM是唯一一家能够提供真正的端到端应用程序安全解决方案的提供商，用来管理开发流程各个阶段的安全合规性——从编码到生产各个阶段。



数据及应用程序安全入门

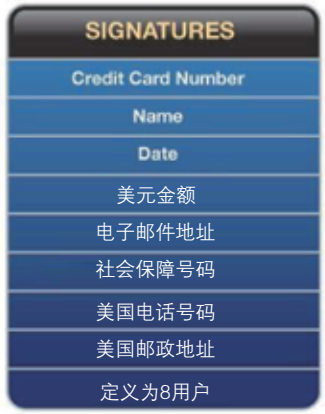
门户安全与联盟

- 合作伙伴服务产生的新的收入
- 合并后快速集成
- 云安全访问控制
- 统一J2EE和.Net



门户安全与联盟

- 检测您网络中PII泄漏情况；
- 封堵不适当的Web和邮件内容；
- 防止已知/未知的网络攻击

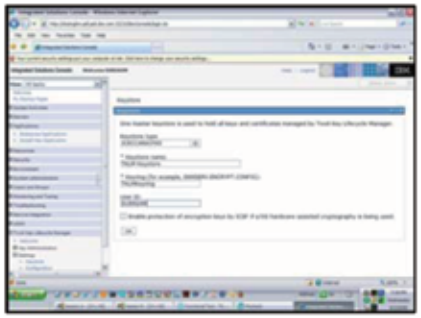


SharePoint/DataPower管理

- 当每个客户端安装多个DataPower/SharePoint时，则需要进行SharePoint/DataPower管理；
- 集中式、一致的策略管理
- 支持合规性及应用程序可用性

存储加密密钥管理

- 适用于PCI及加密规则的经济有效、低OPEX解决方案
- 确保在整个寿命周期内密钥的可用性
- 检测您网络中PII泄漏情况；
- 封堵不适当的Web和邮件内容；
- 防止已知/未知的网络攻击



如何保护您企业关键应用程序与服务的数据访问安全?

企业需要保护客户端及客户PII的访问及披露（例如，信用卡、SSN、患者）记录及财务成果

安全主管

公司内联网

安全架构师

（内部工具）

按照需要进行转译，从而对采取了信息安全策略的所有服务信息进行加密

应用程序所有者

（Eclipse）

转译并编码为特定于应用程序的数据授权策略

IT运营IAM控制面板

转译并编码为配置及特定于工具的访问策略

客户如何向企业证明合规性?

利用Tivoli Security Policy Manager，无需修改应用程序即可集中管理并执行数据访问

企业需要保护客户端及客户PII的访问及披露（例如，信用卡、SSN、患者）记录及财务成果

安全主管

公司内联网

安全架构师

（内部工具）

应用程序所有者

（Eclipse）

IT运营

策略设计工具

Tivoli Security Policy Manager

数据库（DB2、Oracle）

Java、.NET Apps（例如，Portal）

内容管理器（例如，FileNet，SharePoint）

论证合规性及推动数据与应用程序安全

Tivoli Security Policy Manager及FileNet演示

IBM数据及应用程序安全

策略：

交付创新型、整合的新型解决方案来解决关键的合规性及数据保护所面对的挑战

创新与集成的重点领域

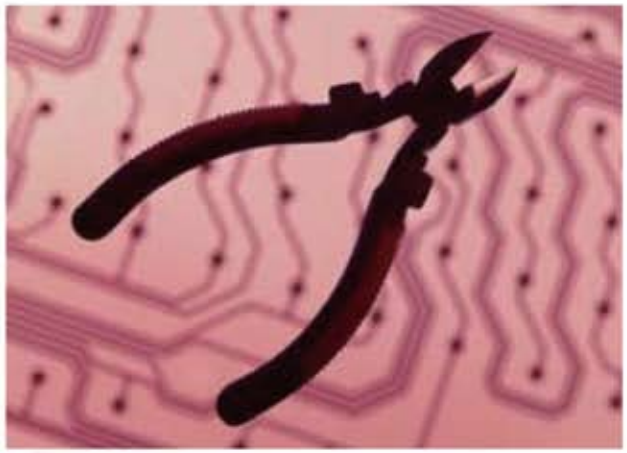
- 内容识别访问控制
- 应用程序安全/内容控制
- 端到端合规性可见性
- 标准的领先地位

市场驱动因素

简化	合规性	云/Web 2.0	应用程序与数据保护

威胁形势不断地变化着。对于企业而言，若要保持与之同步的确是一个挑战

- 对新技术和应用程序（包括虚拟化与云安全）的风险认识不足；
- 寄生、隐秘的有害攻击；
- 无法确立法庭科学证据；
- 由于优先访问权的误用以及事故引发的停机而无法检测破坏行为；
- 管理日渐提高的安全技术所产生的复合成本。



数据中心及运行安全

- 按照SLA的规定，改进服务可用性并支持性能；
- 降低安全运行的长期管理成本；
- 通过降低病毒、蠕虫、有害代码、垃圾邮件侵袭的风险来提高生产效率；
- 深入研究特殊的破坏行为，从而快速获得解决。

了解数据中心及运行安全

网络

服务器

虚拟化

安全事件、日志管理与报告

数据中心与运行安全

（安全的web型工具）

网络防护

IBM安全网络IPS

IBM安全网络IPS

虚拟设备

统一的威胁管理

IBM安全网络多功能

虚拟基础架构保护

IBM Security Virtual Server Protection for VMware

服务器保护

IBM Security Server及Server Sensor

安全管理

托管的安全服务

IBM安全SITEProtector

产品
云安全技术提供商的附加值

网络威胁防护

防止内外部未经授权的侵入行为

漏洞管理

通过精确地识别、确定优先次序、追踪并报告云安全技术基础架构的漏洞来降低风险

服务器与虚拟化安全

多层防护，旨在确保云安全技术数据和应用程序的安全性

托管的安全服务

实时安全管理，包括系统监控、紧急响应和有保证的24/7防护

网络入侵防护

策略：

网络入侵防护系统（IPS）是IBM安全产品组合中一个关键的“着力点”。利用该控制点能够实现新的功能。

创新与集成的重点领域

- 高性能/扩展功能集的开发
- 数据中心内容扩展

市场驱动因素

简化 | 更多安全功能 | 威胁保护 | 应用程序与数据保护

端点（服务器）入侵防护

策略：

服务器安全是IBM安全方面的一个关键的“着力点”。IBM将交付集中式服务器代理，用于确保合规性、配置管理及威胁防护。

创新与集成的重点领域

- 数据中心安全性
- 产品集成与广泛的平台支持
- 虚拟化

市场驱动因素

- 简化
- 威胁与操作覆盖面
- 广泛的平台支持

IBM Security Virtual Server Protection

策略：

使用虚拟服务器安全来消除安全与合规性障碍，这些障碍阻止客户采取虚拟化及云计算

创新与集成的重点领域

Virtual Server Protection for Vmware® 扩展的功能集

虚拟环境、服务器与应用程序是安全的“着力点”。

市场驱动因素

威胁与操作的统一 | 服务器生命周期管理 | 威胁防护 | 合规性

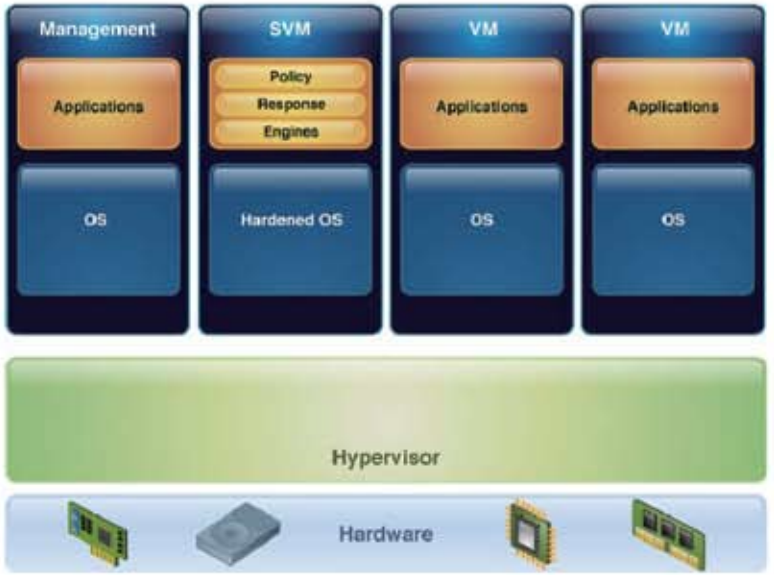
虚拟化面临的安全挑战：新的复杂情况

- 新的情况
  - VM的动态重新部署；
  - 增加基础架构层来进行管理与防护；
  - 每台服务器多个操作系统及应用程序；
  - 消除系统之间的物理界限；
  - 手动跟踪软件及VM配置

虚拟化之前

- 每台服务器的操作系统与应用程序的比率为1：1

虚拟化之后



- 每台服务器操作系统与应用程序之间的比率为1：多；
- 需要管理与保护的其他层

虚拟基础架构保护之所以具有重要性的三个原因

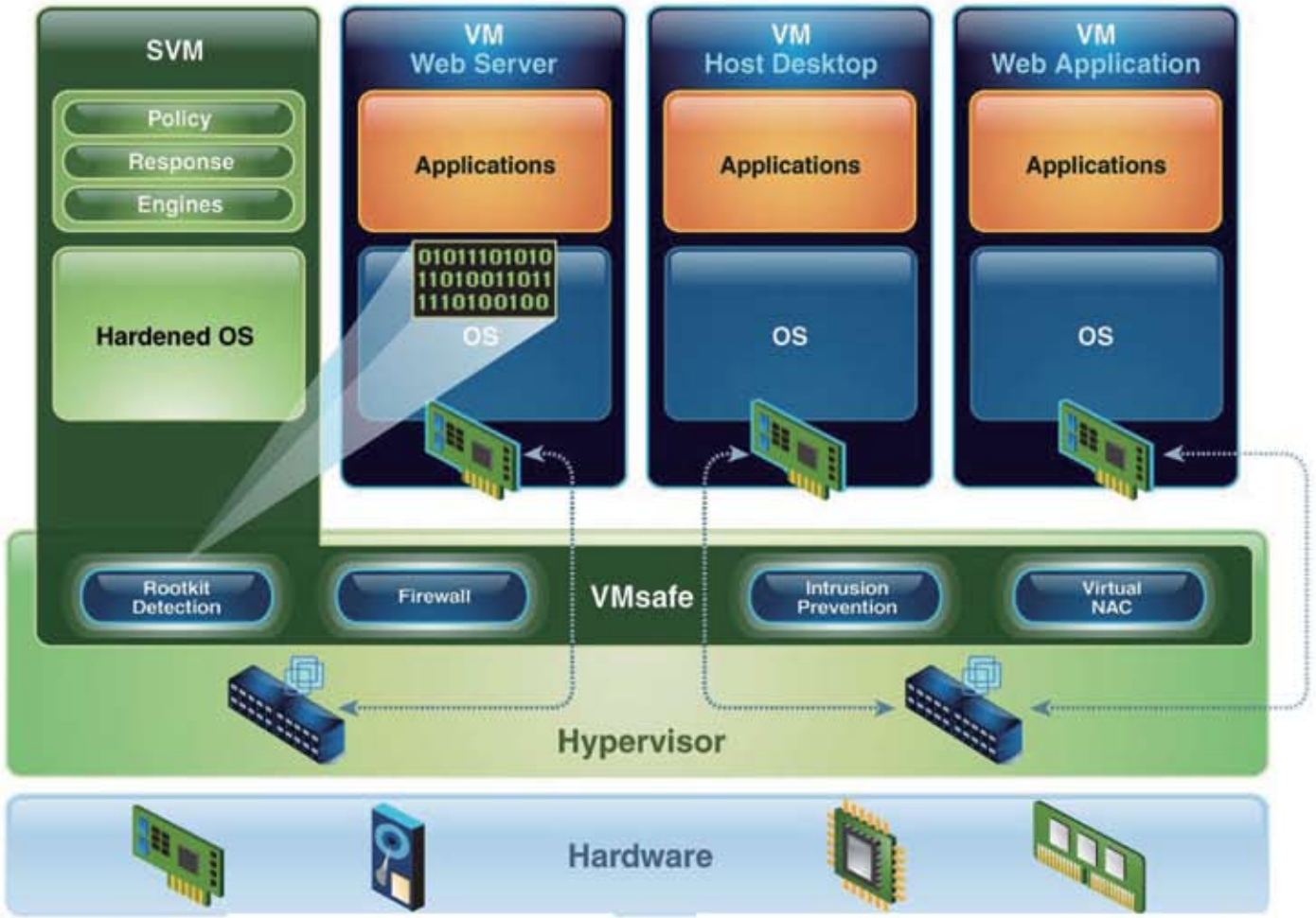
需求	IBM Security Virtual Server Protection for VMware®的功
减轻虚拟化所引入的新风险和复杂性	 为虚拟架构的每一层提供动态保护
保持合规性标准与法规	 通过提供专门为虚拟基础架构定制的安全与报告功能来协助满足合规性要求
驱动运行效率	 提高虚拟基础架构的投资回报（ROI）

虚拟化面临的安全挑战：新风险

引入IBM Security Virtual Server Protection for VMware

针对Vmware vSphere 4的整合的威胁防护

通过为虚拟数据中心交付整合、优化的安全性，从而确保用户更加安全、合规并节约成本



为虚拟基础架构每一层提供动态防护。

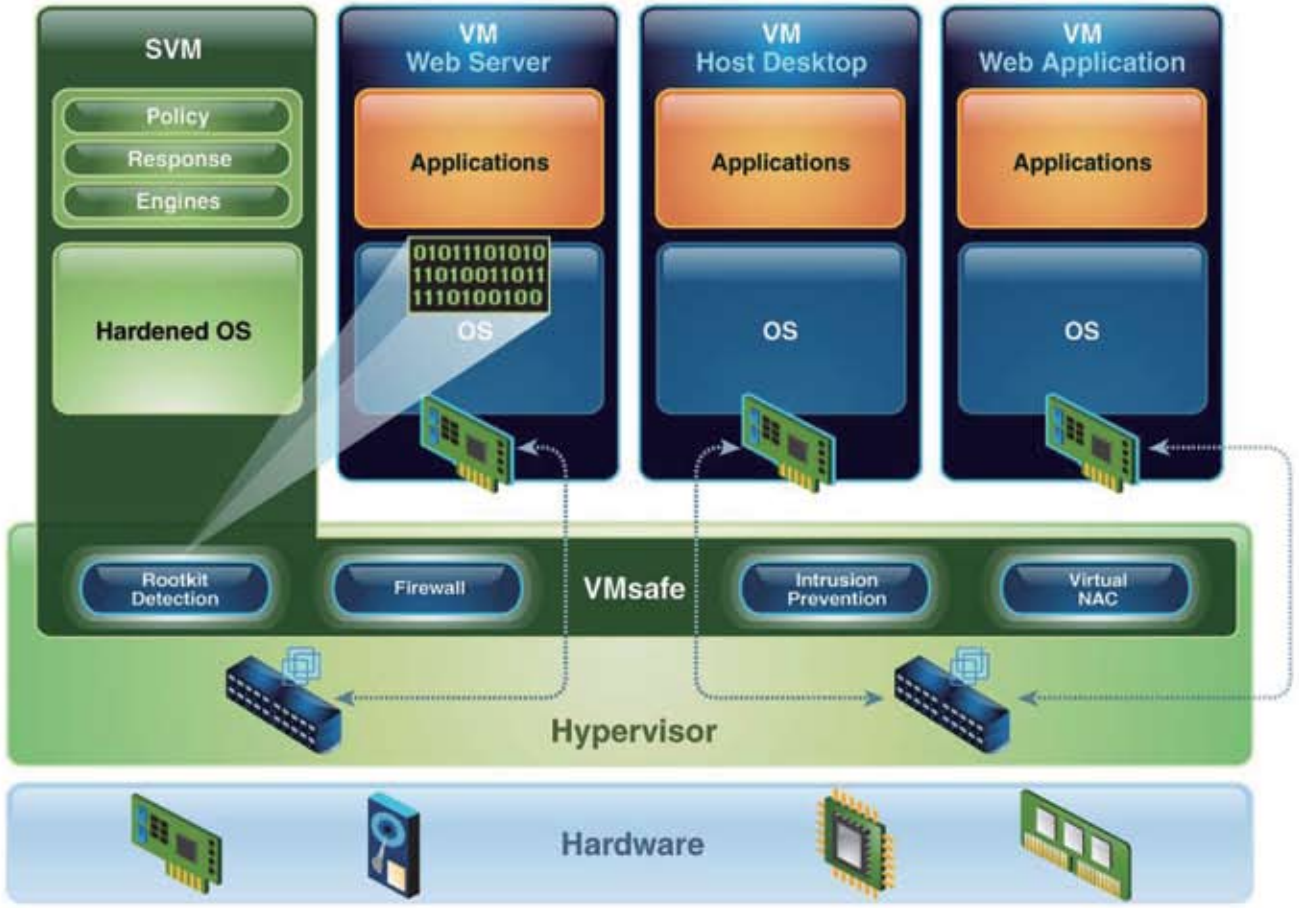
通过为虚拟基础架构提供安全性及报告功能，从而满足合规要求。

利用虚拟数据中心的物理安全性来提高投资回报率。

利用虚拟rootkit检测来提高虚拟服务器的正常运行时间。

Virtual Server Protection for VMware使您能够实现虚拟化优势并且无需降低您的安全防护水平

- 为虚拟基础架构每一层提供动态保护
  - 管理程序
  - 操作系统
  - 网络
  - 应用程序
  - 虚拟机（VM）
  - 虚拟机间通信



IBM：综合安全风险及合规性管理

- 市场中唯一能够提供端到端安全基础覆盖的安全解决方案方；
- 15，000名研究人员、开发人员以及中小企业参与到安全计划中；
- 3，000项以上的安全与风险管理专利；
- 200份以上的安全客户参考以及50份以上的已公开案例研究；
- 在确保zSeries环境安全方面40年以上的成功经验；
- 每天为客户管理70亿以上的安全事件


Thank
You

商标和免责声明

Intel、Intel 徽标、Intel Inside、Intel Inside 徽标、Intel Centrino、Intel Centrino 徽标、Celeron、Intel Xeon、Intel SpeedStep、Itanium 和 Pentium 是英特尔公司及其子公司在美国和其他国家或地区的商标或注册商标。Linux 是 Linus Torvalds 在美国和/或其他国家/地区的注册商标。Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft 公司在美国和/或其他国家/地区的商标。IT Infrastructure Library 是英国中央计算机与电信局（现在隶属于英国商务部）的注册商标。ITIL 是英国政府商务部的注册商标和社区注册商标，已经在美国专利和商标局注册。UNIX 是 The Open Group 在美国和其他国家/地区的注册商标。Java 和所有基于 Java 的商标是 Sun Microsystems, Inc. 在美国和/或其他国家/地区的商标。其他公司、产品或服务名称可能是其他公司的商标或服务标志。本文的信息均按“原样”提供，不进行任何形式的保证。

本文出现的所有客户例子均为了说明这些客户如何使用 IBM 产品，以及他们可能已达到的效果。实际环境成本和性能特征可能会因为客户不同而变化。有关非 IBM 产品的信息是通过这些产品的提供商、他们发布的公告或其他公共可用的来源获得的且不表示 IBM 对这些产品的认可。肥IBM 产品的定价和性能是功过公开发表的信息获得，包括供应商的公告和全球主页。IBM 没有测试过这些产品，不能确认与非 IBM 产品相关的性能、兼容性或任何其他声明的准确性。关于非 IBM 产品能力的问题应该由这些产品的提供商解决。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，怒不另行通知。

一些信息介绍的是预期的未来功能。这类信息不计划用作对任何未来产品的特定水平的性能、功能或交付日程安排的承诺的最终陈述。这类承诺仅在 IBM 产品公告中做出。本文信息旨在传递 IBM 当前的投资和开发活动的信息，竭诚帮助客户进行未来规划。性能数据是使用受控环境中的标准 IBM 基准测试，在度量和预测的基础上获得的。用户实际的性能吞吐量可能会随用户作业流中的多进程编程数量、I/O配置、存储配置以及处理的工作负载等因素的不同而变化。因此，不保证个人用户可以实现与文中描述相等的吞吐量或性能提高。

本文中的价格为建议美国定价，如有变更，恕不另行通知。起始价格可能不包括硬盘驱动器、操作系统或其他功能的价格。如需了解您所在地区的最新定价，请联系您的IBM代表或业务伙伴。

所示照片可能为工程样机。生产模型可能有所变动。

本文件中IBM产品或服务参考资料不暗示它们将在所有国家/地区提供。

国际商业机器公司在美国和/其他国家的商标，可访问http://www.ibm.com/legal/copytrade.shtml查询。