云计算白皮书
2009 年 11 月

IBM 观点:
安全和云计算

目录

简介

云计算是一种灵活、经济且可靠的交付平台，可通过互联网提供业务或客户 IT 服务。云计算资源可以快速部署和轻松扩展，可以“按需”供应所有流程、应用和服务，无论用户位于何处。

因此，云计算让组织有机会提高服务交付效率，简化 IT 管理，并使 IT 服务更好地满足动态业务需求。 云计算能以多种方式实现“两全其美”，为核心业务功能提供可靠支持，同时能够开发新服务和创新性服务。

> 云计算的另一优势在于增强用户体验，而又不增加复杂性。 用户无需了解关于底层技术或实施过程的任何内容。

公共云计算模型和私有云计算模型现均已投入使用。 任何连接 Internet 的人员均可获得公共模型，包括软件即服务 (SaaS) 云（如 IB M LotusLive™）、平台即服务 (PaaS) 云（如 IBM 按需计算™）以及安全和数据保护即服务 (SDPaaS) 云（如 IBM 漏洞管理服务）。

私有云由单个组织拥有和使用。 私有云具有许多和公共云相同的优势，而且拥有私有云的组织具有更多灵活性和控制权。 另外，在高峰流量期间，私有云的延迟性低于公共云。 许多组织将公共云计算和私有云计算整合为混合云，从而同时拥有两种模型。 这些混合云旨在满足特定业务需求和技术需求，有助于以最少的固定 IT 成本投资来优化安全性和隐私性。

云计算的优势显而易见，恰当地保证云计算实施的安全性也迫在眉睫。 下文概述了有关云计算的关键问题，最后阐述了 IBM 对安全的云架构和环境的观点。

解决云的安全问题——重大挑战

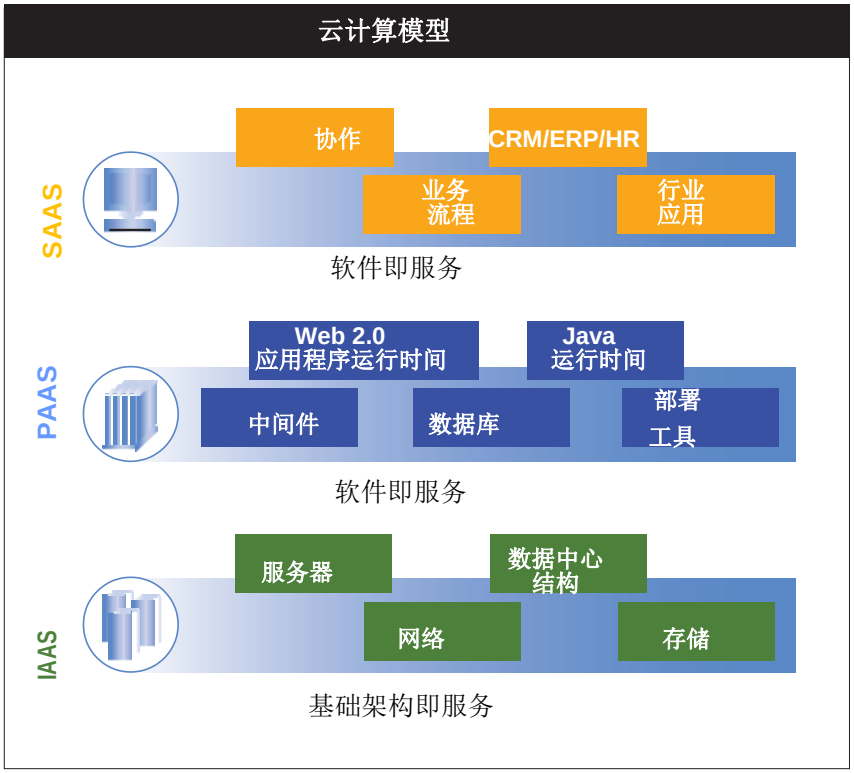
除了常见的开发安全 IT 系统的挑战，云计算还由于重要服务常常外包给第三方而增加了风险。 外包的“外部化”特性使得较难维护数据完整性和隐私，较难支持数据和服务可用性，也比较难证明合规性。

实际上，云计算是将数据和操作的大部分控制权从客户组织转移给了他们的云计算供应商，这种方法类似于组织将部分 IT 操作委托给外包公司。 即使是基础任务（如应用补丁和配置防火墙），也可成为云服务提供商而不是终端用户的职责。 因此，客户必须和提供商建立信任关系，并理解提供商在代表他们实施、部署和管理安全时的风险。 云服务提供商和客户之间的这种“信任但要核实”的关系至关重要，因为即使工作负载转移到云上，最终还是由客户负责关键数据的合规性和安全性。 实际上，由于外包服务存在风险，一些组织因此选择私有或混合模型而不是公共云。

另一方面，云计算也需要重新评估安全和风险。 在云内部，难以定位存储数据的物理位置。 曾经可见的安全流程现在隐藏在抽象层后面。 缺乏可见性会导致许多安全和合规问题。

另外，云计算基础架构的大量分享造成云安全和传统 IT 环境安全之间存在明显差异。 用户横跨不同企业，且信任级别通常与同一计算资源组交互作用。 同时，如今动态 IT 环境的工作负载平衡、服务水平协议 (SLA) 改变等都为错误配置、数据威胁和恶意行为创造了更多机会。

基础架构共享要求较高程度的标准化和流程自动化，这一点有助于消除操作者犯错和疏忽的风险，提高安全性。 然而，分享较多的基础架构本质上存在风险，这就意味着云计算模型仍然需要非常重视隔离、身份和合规。



评估不同的云计算模型

不同的云计算模型通过不同的方法将潜在基础架构呈现给用户。 这会影响对计算基础架构管理的直接控制程度和管理基础架构安全性的责任分配。

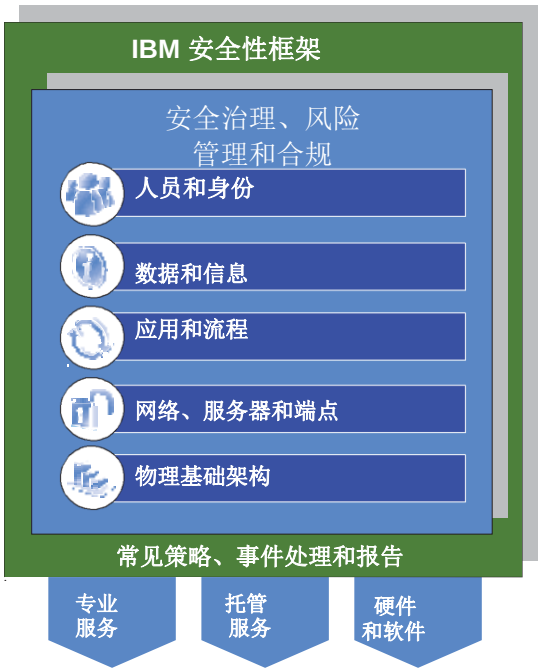
利用 SaaS 模型时，云提供商承担安全管理的大部分责任。 SaaS 提供众多控制 Web 门户访问的方法，比如管理用户身份、配置应用等级，以及限制对特定 IP 地址范围或地理位置的访问。

平台即服务等云模型让客户承担较多责任，管理中间件的配置和安全、数据库软件以及应用程序运行时间环境。 基础架构即服务 (IaaS) 模型将更多控制权和安全责任由云提供商转移给客户。 在此模型下可访问支持虚拟映像、网络和存储的操作系统。

组织对这些云计算模型极有兴趣，因为这些模型非常灵活和划算，但是组织同样关注安全。 业内分析师进行的最新云计算采用情况研究和出版文章证实了这些问题，比如缺乏可见性和控制力，如何在共享、外部管理的环境中保护敏感信息和存储受管信息等。

对关键 IT 服务而言，距离大量采用外部的、大规模共享和完全开放的云计算平台仍需几年时间。

近期，大多数组织都在寻找充分利用外部云计算提供商服务的方法。 这些云主要用于配置文件风险较低的工作负载，在其中缺乏保证的一体适用的安全方法是可以接受的，且其中价格为主要的差异化优势。 如果工作负载的配置文件具有中到高级别的风险且涉及高标准或专利信息，那么组织会选择可提供较高控制和安全保证的私有云和混合云。 随着外部云开始提供更紧密、更灵活的安全性，这些工作负载会逐渐转移到外部云。



检查 IBM 安全性框架

IBM 安全性框架是为描述需要保护的业务资源的安全性而开发的，它从业务角度来查看不同的资源域。

根据 IBM 安全性框架以及与 IBM 客户进行的大量讨论，下文提供如今企业级云计算的主要安全性需求清单。（要获得更多信息，请参考《IBM 安全性框架和 IBM 安全性蓝图，实现业务驱动安全性》， IBM RedGuide REDP-4528-00，2009 年 7 月。）

安全治理、风险管理和合规

组织需要看见云的安全性状况。 这就包括变更、映像和事件管理的普遍可见性，以及租户、针对租户的日志和审计数据的事件报告可见性。

可见性对合规尤为重要。《萨班斯-奥克斯利法案》、《健康保险流通与责任法案 (HIPAA)》、欧洲隐私法和其他许多法规都要求全面审计功能。 由于按照定义，公共云对订阅者而言为“黑盒子”，因此潜在的云订阅者可能无法验证合规性。（另一方面，私有云或混合云可通过配置来满足这些需求）。

另外，有时需要提供商支持第三方审计，当被怀疑违规时，他们的客户可被要求进行电子发现和法庭调查。 这使得维护合适的云可见性更加重要。

一般来说，根据组织在战略外包和传统、托管服务方面的经验，他们通常需要可适应具体情形的灵活 SLA。

人员和身份

组织需要确保整个公司和供应链的授权用户可以访问所需数据和工具，而且组织可以在需要时阻止未授权的访问。 云计算环境通常支持众多的用户社区，因此这些控制更加重要。 另外，云计算引入了新的特权用户层：为云计算提供商服务的管理员。 特权用户监控（包括记录活动）成为一项重大需求。 这种监控应包括物理监控和背景检查。

必须支持身份联合和快速入职功能，利用企业后端或第三方系统协调身份验证和授权。 需要以标准为基础的单点登录功能来简化内部托管应用程序和云计算最终端用户注册过程，让最终用户可轻松快捷地充分利用云服务。

数据和信息

大多数组织将数据保护作为他们最重要的安全问题。 常见问题包括数据存储和访问方式、合规和审计要求以及业务问题（包括数据泄露成本、通知要求和品牌价值损坏）。 在云存储基础架构上需要正确分割所有的感数据或规定数据（包括存档数据）。

将转存到云中的数据或闲置在服务提供商数据中心的数据进行加密，并管理加密密钥，这对保护数据隐私和遵从合规要求非常重要。 对移动数据进行加密，并在云服务提供商和客户之间分享这些加密密钥，是一项重要但通常被忽视的需求。 由于在许多情况下，通过 Internet 快速经济地移动大量数据仍不切实际，因此许多组织不得不将移动媒介（如存档磁带）发送给云计算提供商。 将数据加密，并且只有云提供商和客户可以获得加密密钥，这点非常重要。

根据组织位置、所处理的数据类型和业务特性，在利用云计算时会产生明显的数据分配限制。 例如，一些欧盟成员明令禁止其公民的非公开个人信息离开国境。

> 美国一些州政府不允许将其员工的非公开个人信息发往国外。

另外，云部署可产生与加密信息输出有关的违法问题，且这种部署可能使知识产权面临严重威胁。 公司的法律顾问必须在部署云计算之前全面审查所有这些需求，确保组织持有对数据在提供商基础架构中的地理位置的控制权。

如果一些领域的用户和数据具有明确指出的不同风险类别（比如公共服务和财政服务），那么组织需要维护云数据的分类。 数据分类将会监管谁访问了数据、数据的加密和存档方式，以及如何使用技术防止数据丢失。

应用和流程

客户通常从映像安全方面来考虑云应用的安全性需求。 所有的常见应用安全需求仍适用于云计算中的应用程序，但这些安全需求也适用于托管这些应用程序的映像。 云计算提供商需要遵循和支持安全的开发流程。 另外，云计算用户需要支持映像起源以及许可和使用控制。 必须小心执行映像暂停和破坏，确保这些映像中包含的敏感数据不会被暴露。

确定、验证和维护映像的安全状况与针对客户的安全策略，这项需求很重要，尤其是在高度标准化的行业中。 组织需要确保他们发布到云中的 Web 服务是安全的、相同的且能满足企业策略。 充分利用安全开发的最佳实践是一项重要需求。

网络、服务器和端点

在共享云环境中，客户希望确保所有的租用域得到正确隔离，并且数据或事务不会从一个租用域泄漏到另一个。 为实现这一点，客户需要能够配置受信任的虚拟域或基于策略的安全域。

随着数据进一步脱离客户的控制，客户希望能够对将要构建到环境中的系统进行入侵检测和保护。 问题不仅在于入侵客户的信任虚拟域，还在于保护数据不被泄露和“挤出”（也就是说，错用客户域而加载对第三方的攻击）。 将数据移动到外部服务提供商还会引起其他问题：内部和 Internet 服务拒绝 (DoS) 或分布式服务拒绝 (DDoS) 攻击。

由于信息安全为移动式目标，必须定期审查环境，防止常见威胁和漏洞。

在共享环境中，有关各方必须对审查数据和定期执行审查的责任达成一致。 组织必须在合同管理上处于领导地位，重新评估风险或控制未直接参与执行的部署。

若映像目录由云计算提供商提供，客户会希望这些映像是安全的且得到正确保护，不会被破坏和滥用。 许多客户希望这些映像通过密码验证和保护。

物理基础架构

云计算的基础架构（包括服务器、路由器、存储设备、电源和其他支持操作的组件）在物理上应该是安全的。 防护措施包括使用生物计量访问控制措施和闭路电视 (CCTV) 监控来充分控制和监控物理访问。 提供商需要明确解释物理访问如何托管给服务器，服务器可托管客户工作负载并支持客户数据。

了解 IBM 关于云安全的观点

IBM 根据在一系列垂直行业中设计、实施和支持云计算解决方案的经验，提供了关于云安全的明智观点。

安全不存在“一体适用”

不存在“一体适用”的云安全模型。 组织具有不同的安全需求，这些需求由组织想要迁移到云中的业务工作负载的独特性质所决定。

组织对云环境和企业后端系统具有许多不同的整合需求。 一些组织正在开发全新的应用，并准备将他们的云环境构建成与任何现有操作均不相关，但大多数企业客户开始采用混合云或私有云，其中核心需求为与企业系统相整合。

在这种情况下，现有安全管理基础架构可轻松整合到云中，尤其是联邦协议的使用，这些都能很好地促成云计算的成功部署。 比如 OpenID 和安全性断言标记语言 (SAML) 等身份联盟协议会受到众多关注，且在公共云中扮演着重要角色，但是在企业中需要支持众多其他协议。 这些协议均是为了快速将数据从企业后端系统移动到私有云或混合云中。

不同类型的工作负载需要不同级别的安全性。 最重要的需求之一是第三方安全审核或验证，政府甚至需要正式验证和身份认证。 身份证明的强度（确保登录服务的人真的是如他们所声称的那样）和身份验证机制的强度根据工作负载类型的不同而不同。 因此要设置用于核实身份的全新公开服务，提供不同的服务质量登记。

加密需求因客户而异。 一些客户强烈要求使用特定密码算法，且对访问密钥的人员有很严格的限制，而另一些客户则只需对特定数据进行加密，且希望将重要的管理委托给受信任的云服务提供商。

可用性要求有重大变动，包括允许提供商做出响应并从故障中恢复的时间。 在执行安全和合规检查期间，需求也不同。

IBM 的观点是企业级云服务的提供商必须支持一系列安全和服务级别选项，同时支持可扩展且基于行业标准的安全基础架构，使其很容易与现有操作相整合。 另外，服务提供商必须根据需要与客户的云安全功能相整合，并扩展这些功能。


典型的云服务层
所交付的云服务
软件即服务 应用软件经许可作为服务，按需向客户提供。
平台即服务
优化的中间件 – 应用服务器、数据库服务器、门户服务器
基础架构即服务
虚拟服务器、存储、网络
云平台
业务支持服务
服务管理、客户管理、订单管理、账单
运营支持服务 基础架构配置、实例、映像、资源/资产管理
虚拟资源
虚拟网络、服务器、存储
系统资源
网络、服务器、存储
物理系统和环境

一种用于云计算的基础架构模型

一种用于云计算的基础架构模型由分层服务的堆栈所组成。 物理系统层描述常见的数据中心要求，命令执行访问控制措施，并监控设施。 系统资源层监管网络、服务器和存储基础架构。 虚拟资源层引入强制隔离，作为虚拟安全的核心性质： 通过虚拟机管理程序和数据分离来隔离程序。

接下去的层是确定云管理平台的运营支持服务 (OSS) 和业务支持服务 (BSS)。顶部为各种云交付服务，包括基础架构即服务、平台即服务和应用程序即服务。

该架构的各层均存在安全需求，关键在于维护各层之间的一致性。 例如，如果最高堆栈等级的安全策略确定客户信息无法离开国家，那么必须在国内分配较低等级的物理资源、磁盘空间，用来存储这类客户信息。


典型的云服务层
所交付的云服务
软件即服务 应用软件经许可作为服务，按需向客户提供。
软件即服务
优化的中间件 – 应用服务器、数据库服务器、门户服务器
基础架构即服务
虚拟服务器、存储、网络
云平台
业务支持服务
服务管理、客户管理、订单管理、账单
运营支持服务 基础架构配置实例、映像、资源/资产管理
虚拟资源
虚拟网络、服务器、存储
系统资源
网络、服务器、存储
物理系统和环境
SOA 安全性
身份
合规
隔离
• 联合身份、身份验证、授权
• 审计和合规报告、入侵检测和防护
• 订阅者域的安全隔离，与现有企业安全基础架构的安全整合
保障虚拟运行时的安全
身份
• 控制特权用户访问（提供商管理、订阅者管理）
• 有效的订阅者入职
合规
• 基于策略的方法
• 多租户日志管理和遵从性报表
•映像 映像和 VM 完整性、映像起源
隔离
• 程序隔离（尤其是在超级管理程序/VM级别）
• 安全和位置约束条件的配置
• 数据隔离、数据加密
• 多租户安全服务

云安全和 SOA
此处所述的云架构让我们可以构建非常简单的云安全模型，由以下两个主要概念组成： SOA 安全层——寄存在新安全虚拟运行时间层的顶部。

云交付服务层是一种复杂的分布式 SOA 环境。 在企业中，不同的服务可分布在不同的云上。 服务可能位于不同的管理或安全域中，这些安全域连接在一起，形成一个云应用程序。 SOA 安全模型完全适用于云。 Web 服务 (WS) 协议堆栈形成 SOA 安全的基础，也因此形成云安全的基础。 整个 IBM 软件堆栈中完全支持这种安全模型。 （要获得更多关于这些产品和 SOA 安全模型的信息，请参考 IBM Redbook SG24-7310-01）。 IBM Tivoli® Federated Identity Manager 这类解决方案为连接各种安全域提供宽泛的、基于标准的支持，使用户可无缝地获取云服务。 在试着将内部 IT 资源和第三方云服务一起构建在混合云模型中时，或将若干第三方服务封装在一个品牌服务产品中提供给客户时，这一点尤其重要。

SOA 的关键功能之一在于它能够轻易整合来自不同提供商的不同服务。 由于云计算有时支持非常多的租户、服务和标准，因此相比大多数企业 SOA 环境，云计算将这种模型更加往前推进了一步。 以高度动态和敏捷的方式且在极为复杂的信任关系下提供这种支持。 特别是，云 SOA 有时支持大量开放用户，且无法假设云提供商和订阅者之间的预设定关系。

许多云计算的实施过程关注特定协议（比如身份联盟的 OpenID），且倾向于特定架构风格（比如具象状态传输，REST）。 IBM 的观点是：企业级云计算不能将其用户限定于特定协议或风格，而是要具有灵活性和多项选择。 虽然 IBM 支持基于 REST 的合适接口和协议，但是 SOA 安全仍需要如 SOA 安全性参考模型中所述的大量安全服务。

SOA 中有一个基本概念，即，将安全体现为服务，且这些服务可通过其他服务来使用。

在云服务中，为了确保正确的用户获得正确的资源，基于标准的证明、登入和用户身份验证只是冰山一角。 为确保云服务的所有潜在组件可维持数据隐私并坚持进行合规性监管，需要用于授权和访问控制的一致性策略。 例如，医疗研究应用从多个医院的诊疗和账单服务中抽取数据，因此必须将病人姓名和其他个人身份信息从全部来源中消除。 集中式的授权管理服务（比如 IBM Tivoli Security Policy Manager）有助于确保定义和执行公共策略，保护所有云服务中的患者隐私。

云计算提供商可在云内和云之间支持 SaaS 和 IaaS。 提供商应坚持实施最佳实践，并为客户提供对安全和云服务的合规状况最大程度的可见性。 IBM Rational® AppScan® 组合有助于支持应用的安全。 IBM Tivoli Security Information 和 Event Manager 可提供安全审计日志和预包装报告的整合视图，用于证明合规工作和特权内部用户的身份威胁。 监控特许 IT 管理员引起的威胁并对此做出反应的能力在公共云模型中显得尤为重要，这是因为在公共云模型中，第三方管理员可获得许多不同组织的数据。

底部的安全虚拟运行时间层是一种虚拟系统，运行可访问数据商店中的数据的程序。 这种运行时与常规的运行时系统的不同之处在于其在虚拟机映像上工作，而不是在个别应用上工作。 它提供诸如杀毒软件的安全服务、自我检测以及虚拟映像周围的外部安全服务。

虽然安全虚拟运行时间的基础早于 SOA 安全，且根据几十年的主框架架构经验而建立，但安全虚拟运行时间的开发仍在不断变化。 IBM 不断投资，研究和开发网络、服务器、超级管理程序、流程和存储基础架构等所有层的较强隔离，从而支持大量租户。

配置虚拟资源，可强制执行安全域和位置限制。 必须根据策略将虚拟资源分组，自动管理安全配置也有助于确保一致性。

在安全虚拟运行时内部，安全服务也通过 SOA 服务不断具体化，提供了身份、审计、关键管理、策略和其他服务。 IBM Proventia® 虚拟网络安全平台是一个可扩展的虚拟安全平台，可提供入侵保护、Web 应用保护和网络策略执行等威胁管理功能。

简化安全控制和防御的机会

虽然人们通常认为云计算增加了安全风险且引入了新的威胁，但云计算也呈现了提高安全性的极佳机会。 标准化、自动化以及基础架构的可见性增加等云特性都会迅速提升安全等级。

例如，使用一组经定义的云接口以及集中身份和访问控制策略，这都会降低用户访问不相关资源的风险。 在隔离域中运行计算服务、默认情况下加密移动数据和限制数据，以及通过虚拟存储控制数据，这些活动都可提高可审计性和减少数据丢失。 另外，自动配置并重新声明已经固化的运行时映像可减少受攻击面并提高取证能力。

全球 IBM 研究人员、开发人员和安全专家已荣获 3,000 多个安全和风险管理专利。

IBM 在驱动业务创新和保证所有风险域的操作流程的安全方面具有无与伦比的能力。 它拥有全面的解决方案和服务，可让组织降低企业内部的安全复杂性，并实施整体的安全管理战略。

借助 IBM，组织可在企业中开发全面、可扩展、基于标准的解决方案，支持目前及未来几年的安全需求。

更多信息

要了解更多关于云计算安全的内容，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问 ibm.com.cn。

读者也可咨询云安全指南，IBM 对云安全实施方案的建议 (REDP-4614)。 这份 IBM RedGuide 提供了更多关于云保护、威胁回应和事件管理职责方面的信息。

以下网站可找到更多关于云安全的信息：

IBM 云计算：http://www-01.ibm.com/software/cn/tivoli/solution/cloudcomputing/

IBM 企业安全性：ibm.com/security

IBM Internet 安全性系统：ibm.com/services/security

IBM X-Force® 安全性提醒和咨询：xforce.iss.net

此外，IBM Global Financing 能根据您独特的 IT 需求定制财务解决方案。如需了解有关优惠信息、灵活的支付方案和贷款、资产回购和转让的更多信息，请访问：**ibm.com**/financing

在美国印刷
2009 年 11 月

TIW14045-CNZH-01