# 云**计算调研报告--云计算真的安全吗？**

摘要：云计算目前是IT行业中非常火热的概念和方向。大型科技巨头正在为各个行业提供云服务，因为保护架构和企业数据是他们的基本政策。在云基础架构中，企业的网络安全问题是数字化转型面临的最大挑战之一。在这种大数据的时代下，云计算真的安全吗？无服务器计算方面更侧重于保护网络安全服务和策略，这有助于防止数据泄露、网络攻击和其他不寻常的网络盗窃活动。

调研的问题：云计算真的安全吗？

调研的目的：探讨云计算是否安全。

调研的意义：让我们能够信赖云计算。

调研方法：查阅资料总结。

一、什么是云安全？

“云安全”是继“云计算”“云存储”之后出现的“云”技术的重要用，是传统IT 领域安全概念在云计算时代的延伸。

云安全的内涵：包括两个方面:一是计算安全；二是安全云。

计算安全：通过相关安全技术，形成安全解决方案，以保护云计算系统本身的安全。

安全云：特指网络安全厂商构建的提供安全服务的云，让安全成为云计算的一种服务形式。

云安全与传统安全：随着传统环境向云计算环境的大规模迁移，云计算环境下的安全问题变得越来越重要。相对于传统安全，云计算的资源虚拟化、动态分配以及多租户、特权用户、服务外包等特性造成信任关系的建立、管理和维护更加困难，服务授权和访问控制变得更加复杂，网络边界变得模糊等问题让“云”面临更大的挑战，云的安全成为最为关注的问题。

二、云计算中的数据安全问题：

云计算为用户提供了非常健康的服务，由于安全限制，许多企业不支持云计算服务。

数据安全和隐私保护是大家所关心的问题。这种安全困境阻碍了管理者、客户加强云计算技术提供的服务。使用任何云服务之前，客户和云提供商之间应该建立一种信任关系。

云计算架构框架整合了许多风险。其中一些是：法律法规；虚拟化风险；严格的网络政策。云计算是客户使用云服务的虚拟环境。它将向云提供数据，而无需获知数据的物理位置。存储提供商必须具备的基本条件是机密性、完整性和可用性。

云的模型应该使用特定的隐藏参数来实现，包括：防火墙限制、强大的网络策略、入站/出站跟踪、数据的加密和解密等。

三、云数据安全关键参数

在当今基于云的数字化转型中，客户正在寻找一个平台来采用云框架/服务来进行数据存储管理和物理存储安全计算。在云平台中，保护所有这些参数对于 CSP 和架构师至关重要，他们负责设置整个环境。此外，除了安全性之外，服务成本也是许多云服务用户（客户）面临的另一个问题。因此，在任何云平台上部署软件模型之前，都应考虑成本和安全合规性。

1.在数据迁移到云之前进行加密；2.使用云加密限制和保护访问；3.限制用户访问；4.本地备份云平台数据；5.云提供商端加密；6. 最大化网关的安全策略。如果不使用云平台提供的云加密策略和服务，则需要客户端或用户在将数据转移到云端之前自行对数据进行预加密。它帮助客户和服务提供商处理某种特定的云业务。云加密是保护计算机的另一种方式。Azure 等云计算服务提供商使用加密技术在系统级别提供一层数据安全性，并允许任何需要共享云服务的人都能安全访问。用户限制也是在云期间评估的关键限制，因为未经授权的访问可能会泄露企业的关键数据到外部世界。企业应通过建立强大的数据防护策略来保护数据。云端加密使用客户端安全服务，这些服务将被整合。云端预定义服务将应用于客户端的数据进行处理和进一步移动。在云平台的服务器端，将会使用数据加密密钥 (DEK) 和密钥加密密钥 (KEK)。这些服务将对迁移的数据进行加密和解密。数据将被加密并以加密格式存储在侧服务器上。如果发生数据泄露或从云服务器被黑客入侵，黑客无法纠正或识别数据。当客户端从服务器访问数据时，数据将被解密并向客户端显示识别的检索输出。网关包含防火墙规则和策略，防火墙规则越多，云数据的安全性就越高。

将业务迁移到云端的企业必须承担新的责任，开发新的技能，并实施新的流程。而改善云计算的安全性的第一步是假设没有安全性。云计算改变了企业的工作方式，并将继续颠覆传统的商业模式。机会和风险都将成倍增加。企业正在将其数据存储在第三方的服务器中，虽然可以控制，但仍然由第三方拥有。即使云计算服务提供商的环境具有高度安全性，但云中的内容（应用程序和数据）仍由企业自己负责。企业的数据移动到云平台中，超出了传统的边界，导致攻击面扩大。随着越来越多的敏感信息存储在云平台中，云平台中的资源越来越成为网络犯罪分子的攻击目标。随着企业的业务向云端迁移，他们将不得不承担新的责任、开发和调整流程，以应对众多未知的威胁。

以下五种最佳实践来保护其公共云的采用：1.了解自己的责任；2.整合合规性；3.自动化防御；4.尽早保护环境；5.实施内部部署学习。云计算的安全性基于共享责任模型。云计算提供商有责任保护物理网络并确保基础设施的安全，而企业有责任保护自己的数据、应用程序和内容（包括用户访问和身份等元素）的安全。合规性是下一代云计算安全服务需求的主要驱动力之一。确保遵守新法规和即将出台的法规的唯一方法是在企业的日常经营中整合法规遵从性，还要考虑网络拓扑的实时快照和对策略更改的实时警报。而站在审计员的立场上，考虑一下他们在审核网络时要求的所有项目，并将这些报告积极地纳入日常工作中。自动化是云计算安全性的关键组成部分。安全审核、控制、补丁和配置管理，所有这些都可以实现自动化，并且可以帮助降低风险。只要有正确的工具和流程，自动化就可以显著地降低人为错误的风险，这对于大规模管理变更至关重要，还可以防止安全漏洞的产生。安全、自动化的云平台可以帮助实时监视网络，并为企业提供快速响应威胁的能力。对于组织而言，即使在开发和质量保证（QA）环境中，也必须保持严格的安全控制。通过在应用程序开发中嵌入适当的控件，早期采用者正在生命周期的早期引入安全性。新的安全性方法促进了按设计安全的理念，即使在开发过程中也要检查源代码是否存在漏洞。无论企业采取何种安全措施，需要确保在内部环境中也采用类似的方法。与传统的本地网络一样，在云平台采用相同的方法也很重要。对于企业来说，使用防火墙、服务器和端点保护解决方案保护网络，服务器和端点的安全至关重要。这些解决方案可以监控企业的流量，防止未经授权的访问并保护企业在云平台中的数据资产免遭破坏、感染或数据丢失。端点和电子邮件安全性使企业的设备保持最新状态，同时防止未经授权访问云计算帐户。当企业将业务迁移到公共云时，必须保持自己的内部部署体验。

网络进程在不断加快，更强更方便的云计算也将比想象中更快的取代传统IDC。因为互联网的存在，这个世界总是充满惊奇，但是凡事有利则有弊，云计算服务虽然大大减轻了用户的成本，但是在其他方面仍然有不可规避的风险。

隐私方面；2.网络传输问题；3.虚拟化安全问题；4.数据集中的安全问题；5.云平台可用性问题；6.云平台遭受攻击的问题。对于用户而言，隐私是一大问题。用户的数据是统一存放在云服务提供商那里的，云服务提供商能够看到每家公司的信息，对于用户而言，如何保证这些数据不被别人恶意利用就成了一个非常大的问题，这需要技术部门的不断完善才行。云计算服务主要是依托网络的，一旦网络运行不稳定，那么对云计算服务影响也是非常大的。虚拟化的可扩展性有利于加强在基础设施、平台、软件层面提供多租户云服务的能力，但虚拟化技术也会带来一些安全问题：如果物理主机受到破坏，其所管理的虚拟服务器由于存在和物理主机的交流，有可能被攻克，若物理主机和虚拟机不交流，则可能存在虚拟机逃逸的情况。云计算系统与用户的数据存储、处理、网络传输等都有关，包括怎么有效存储数据，避免数据丢失或损坏；怎么避免数据被非法访问或者被无故篡改；怎么对多租户应用进行数据隔离；怎么避免数据服务被阻塞等。当云平台遭受攻击时，用户的数据和业务应用将依赖于云平台服务连续性、SLA和IT流程、安全策略、事件处理和分析等。另外，当发生系统故障时，如何保证用户数据的快速恢复也成为一个重要问题。

1. 结论

在调查情况下，云计算的安全性还不错，值得我们信赖和利用。云计算平台的用户、信息资源的高度集中，比较容易成为黑客攻击的目标，因此由于服务造成破坏性将会大大超过传统的企业网络应用环境。尽管云计算是技术上的重大变化，并且看起来可能是一个完全不同的环境，但是安全性的基本原理保持不变。